**South African Intruder Detection Services Association**

# BY-LAW NO. 10

**Communications Standard for Intruder Detection & Visual Verification Systems.**

**APRIL 2022 – Version V2.1**

## 1. GENERAL

1.1 This specification lays down the minimum requirements for the installation of communications equipment accepted for the monitoring of alarm signals in a Central Station/control room. They may include, but are not limited to, Equipment, Cabling, installation and certification of Third-Party Services. 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 client must be clearly informed 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 **Alarm company:** A SAIDSA-approved installation organisation prepared to enter into a contract for the provision of the installation and/or monitoring, reaction and maintenance of an intruder alarm system.

2.1.2 **APN: (Access Point Name)** is the name of a private gateway between a GPRS, IoT or IP communication equipment and the data server for control room transmissions a central station. **(See also 2.1.19)**

2.1.3 **Backup Equipment:**
Essential additional operational central station equipment to be used when equipment failure occurs.

2.1.4 **Central station/control room:** Continually manned premises, equipped to receive and display signals from intruder alarm 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.

2.1.5 **Cloud Server:** This is an on-demand availability of remote data storage, computer system resources and software applications without the requirement to have such items on-site or without active management required by the user. These services may often be distributed over several locations and managed by the service provider on a "pay-as-you-go" model. A cloud server is powerful physical or virtual infrastructure that performs application- and information-processing storage. Cloud servers are created using virtualization software to divide a physical (bare metal) server into multiple virtual servers.

2.1.6 **Communication service provider**
A company providing communication equipment for the purpose of monitoring security systems.

2.1.6 **Control room Transmissions:** The transmission of alarm events from a control panel alarm device to a control room. This can be done through a number of cable or wireless transmission methods including RF, GSM, GPRS, IP, PSTN, DSSS.

2.1.7 **Dual Path Monitoring:**
Two separate communication technologies utilizing alternate communication mediums to transmit signals to a central station/control room. (Refer to 4.1)

2.1.8 **Fibre:**
Fibre-optic internet, commonly called fibre internet or simply "fibre," is a high speed broadband connection with low lag time. The technology uses fibre-optic cable, which can send data as fast as about 70% the speed of light. In addition, fibre-optic cables are not as susceptible to severe weather conditions as other types of traditional cables, which helps minimize outages. It also resists electrical interference effectively. Fibre is ideal for multiple users to connect several devices at once.

2.1.9 **GSM: (Global System for Mobile Communications**) transceivers communicate on a GSM. network and therefore requires coverage from a GSM network to allow communications.
GSM defines the standard for all GSM related protocols (SMS, MMS, Voice, GPRS, EDGE, 3G, etc.). We can identify three main GSM protocols used in the security industry namely Voice, SMS and Data (GPRS, EDGE, 3G, 4G, etc.). The GSM protocols used in GSM transceivers is dependent on the product and the manufacturer/supplier. GSM is inherently secure communications between the subscriber and base station (tower) may be encrypted. GSM networks in South Africa generally has a wide footprint supporting Voice, SMS and Data in almost all regions with increased coverage in metropolitan areas and decreased coverage in rural areas. Security system interface formats include but are not limited to individual inputs, 4x1, 4x1 extended, 4x2, Ademco, Point ID, Contact ID, and SIA. GPRS – (General Packet Radio Service) and SMS (Short Message Service) communicator makes use of the cellular network and is used wherever there is cellular coverage. Most monitored GPRS transceivers utilize a private APN to ensure the security of the bi-directional communication path (secure IP addresses) as well as enabling a secure internet reporting option. A public VPN could be used for additional backup facilities, as well as control functions to the communicator via SMS. GPRS enables Panel up/download and control capabilities. The GPRS and SMS transceivers are available with either single or dual sim.

2.1.10 **High Sites**
High sites are high elevation inner city buildings or outdoor areas with a purpose build building or container to house VHF/UHF, video, two way radio and GSM router equipment.

2.1.11 **Intruder alarm system:** A means of detecting and signalling the presence, entry or attempted entry of an intruder into a protected premise. For the purposes of this By-law, it is specifically noted that the use of wireless/wire free systems is permitted.

2.1.12 **IP: (Internet Protocol)** is the communication format used for internet data communication of control room transmissions.

2.1.13 **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.

2.1.14 **Lora**: A UHF 868MHz band low-power, low data usage IoT technology suitable for information transfer, including status and alarm signals with mainly one-way reporting to servers and base stations. (also sometimes called LoraWan). Lora can be deployed as a private or public commercial network.

2.1.15 **LPWAN: L**ow **P**ower **W**ide **A**rea **N**etwork wireless communication used for bi-directional radio data equipment or modems.

2.1.16 **LTE Cat M:** This is an IoT network based on cellular 4G or 5G LTE networks and suitable for data, status, and alarm signal reporting with 2-way (control) functions possible. This is suitable for fixed or mobile applications (i.e. vehicle tracking).

2.1.17 **Microwave Link:**
A communications system that utilises a beam of radio waves in the microwave frequency range to transmit video, audio, or data between two locations.

2.1.18 **NB-IoT**: This is an IoT network based on cellular 4G or 5G LTE networks and suitable for data, status, and alarm signal reporting with 2-way (control) functions possible. This is mostly suitable for fixed installations.

2.1.19 **Private APN** This is an APN on a private network with improved control and added security over a public network APN. **(See also 2.1.2)**

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

2.1.21 **PSTN**: Private Subscriber Telephone Network or more well-known as a standard telephone line. Although still in use, it is increasingly being replaced with other cabled (Fibre optic) and wireless (typically VHF or GPRS) communications.

2.1.22 **Radio Modems:** Data modems that transfer data wirelessly across a range of up to tens of kilometres, normally through **P**rivate **R**adio **N**etworks (PRN). Private radio networks are used in critical industrial applications like alarm monitoring when real-time data communication is needed and are mostly independent of 3rd party network operators. In most cases users use licensed frequencies either in the UHF or VHF bands. In certain areas licensed frequencies may be reserved for a given user or allocated to be shared for one purpose only, thus ensuring that there is less likelihood of radio interference from other RF-transmitters, ensuring high reliability of data transfer and very high uptime.

2.1.23 **Radio transceiver:** Bi-directional radio equipment with acknowledgement capabilities for the transmission of signals from the protected premises to a central station/control room by radio waves.

2.1.24 **Radio transmitter:** Simplex channel radio equipment for the transmission of signals from the protected premises to a central station/control room by radio waves.

2.1.25 **Redundancy (Communication and Power):**
Refers to the inclusion of additional communication components or equipment that is necessary to take over communication to the control room if the primary communication device has failed.

2.1.26 **Repeater Site:**
Secure site on a mountain range or high rise building that houses VHF repeater equipment.

2.1.27 **Risk Areas -**
**Commercial**: Premises used for the purpose of administration and services e.g. Office or Office Park.
**Industrial:** Premises used for the purposes of Manufacturing, Storage or Distribution e.g. Factory or Warehouse
**Heritage:** Premises such as Museums and Historical Buildings
**Residential:** Premises used for residential purposes e.g. House, Apartment, Housing Estate.
**Retail:** Premises used for the purpose of walk-in sales or displays e.g. Shop
**Government:** Premises such as Government buildings, Municipal, Police Stations, Prisons and Hospitals.

2.1.28 **SAIDSA Requirement/Standard**:
Commercial, Retail, Industrial and high-risk residential installations must have Dual Path monitoring, using different carrier mediums.

2.1.29 **SATLINK:**
A satellite radio link between a transmitting earth station and a receiving earth station through a satellite.

2.1.30 **Sigfox**: A UHF 868MHz band low-power, low data usage IoT technology suitable for information transfer, including status and alarm signals with mainly one-way reporting to servers and base stations. Sigfox is a public commercial network by subscription only and not suitable for private use.

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

2.1.32 **Spread Spectrum:** In radio communication, spread-spectrum techniques are methods by which a signal generated is deliberately spread over a number of frequencies, resulting in a signal that provides more secure communications including increasing resistance to natural interference, noise and jamming.

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

2.1.34 **TCP/IP Modem:** A data modem normally used by connecting an alarm panel directly to a server and central station via GSM, data cable, fibre connection or wireless data connections which may include ADSL, satellite, microwave, SATLINK or fixed LTE connections.

2.1.35 **UHF: U**ltra **H**igh **F**requency is the frequency band used for simplex and duplex (bi-directional) radio communication. Typical examples are UHF alarm transmitters and 868MHz alarm systems, 433MHz and 868MHz alarm, vehicle, gate and garage remotes. This covers all radio transmissions from 300MHz to 3,000MHz (or 3GHz) and can include alarm PIR and handheld remote communication.

2.1.36 **UHF LPWAN transceiver**: This includes **Lora**, **Sigfox**, **NB-IoT** and **LTE Cat M** which are all operating as Low Power Wide Area Networks and between 700MHz and 900MHz. These are typical new IoT type radio modems. While Lora and Sigfox have data volume limitations, NB-IoT and LTE Cat M1 are unlimited formats.

2.1.37 **VHF:**
**V**ery **H**igh **F**requency is the frequency band used for simplex radio communication. Typical examples are alarm transmitters and two way voice radio communication. This covers all radio transmissions from 30MHz to 300MHz.

2.1.38 **VHF Transmitter**:
Long range transmitters are used to communicate on a radio frequency allocated by ICASA and are licenced for distances of 50 km radius and further.
These transmissions may also be relayed via repeaters to increase coverage or to assist in providing communications coverage in areas where direct transmissions are not possible or reliable e.g., out of valleys and behind mountains.
This type of communication is unidirectional, typically from site (client) to the central monitoring station. VHF transmitters can also be routed via GPRS. Once the VHF signal is received by the repeater, it is linked into a GPRS modem that communicates with the central monitoring station where it is received by a GPRS modem and the alarm activation is sent to the central monitoring station computer software. This serves to link multiple monitored areas that cannot be directly linked via VHF to one central control station.

2.1.39 **Visual Verification System:**
Visual verification refers to the use of camera images which are captured at the site of the alarm activation and transmitted in real time via the security system. They offer no distinct detail, but simply evidence of the presence of human activity or movement at the source of the alarm.

## 3. COMMUNICATIONS MEDIUMS

The following methods are considered acceptable. Use can be made of one or more of the following. Dual Path monitoring using different technologies or carrier mediums is recommended.

- Radio Modems
- VHF Radio Transmitters
- UHF Radio Transmitters,
- GSM radios and modems
- UHF LPWAN transceiver
- TCP/IP Modem
- PSTN

## 4. Dual Path Monitoring

4.1 Two separate communication devices must be used, utilizing alternate communication technologies and mediums to transmit signals to a central station/control room that will avoid both devices being affected by a singular event or sabotage attempt. The communication must link directly to the base station, or not utilizing the secondary medium for system routing where possible.

4.2 Retail, Commercial, Industrial or High-risk residential installations cannot be issued with a COC if dual path monitoring is not used for monitoring of the alarm installation.

4.3 In high risk installations it is recommended that the 2nd unit be a self-contained, self-powered device consisting of at least 4 telemetry outputs monitoring tampers, loss of panel, burglary and panic

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

## 5. High Sites

5.1 High site equipment must be monitored in the control room for AC Fail/restore, battery low/restore and hour test signals.

5.2 The repeater site building must be alarmed and any access monitored via a suitable communications medium to the control room.

5.3 **A repeater site data file must be kept and updated regularly and contain the following:**

5.3.1 Name and location (address or co-ordinates) of each repeater.

5.3.2 Names and telephone numbers of the key holders of the repeater site if the site is managed by a high site provider.

5.3.3 Name and 24 hour contact number of person , within the company, responsible for the support and maintenance of the repeater/s.

5.4 **Access to the repeater site must be logged in a log book, consisting of:**

5.4.1 The date and time of the site access

5.4.2 Technicians name

5.4.3 The details for site visit, including the work done.

5.5 It is recommended that very remote high sites have alarmed perimeter monitoring and video surveillance.

## 6. GSM

6.1 GPRS communication is to revert to a second network, when low signal strength or a poor data connection restricts communication.

6.2 No pre-paid SIM cards will be permitted for communication.

6.3 Clients monitored by GSM equipment should be clearly informed in their contract that they are being monitored by GSM technology as well as any risks associated with the connection of this equipment to the cellular network.

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

## 7. Backup equipment / Services

7.1 Backup equipment is to be installed but stay disconnected in the equipment rack in the control room or equipment room.

7.2 Dedicated replacement base station equipment is to be available, per technology and frequency channel or channel set.

7.3 Backup equipment should be clearly marked per frequency or channel of operation.

7.4 A single unused wideband VHF dipole antenna must be available for backup in the event of antenna failure.

7.5 Backup base stations to be started up and tested on a 6 month basis and the battery quality checked.

7.6 **Backup equipment requirements for the monitoring technologies used are:**

- **VHF Transmitter** – Backup base in control room server rack
- **VHF Repeater** - Backup repeater on site, control room or technical support
- **GPRS Base** - Backup base in control room server rack
- **VHF Spread spectrum** – Backup RF link base or Fibre, LTE, satlink, microwave failover connection
- **UHF LPWAN** - Fibre, LTE, satlink, microwave failover connection

## 8. Cloud Servers

8.1 Where cloud servers are used by either the Alarm company or Communication service provider adherence must at all times be given to the provisions of the POPI Act with specific reference to the transfer of personal information outside of the RSA.

8.2 **In particular it is the duty of the Alarm company or Communication service provider, as the case might be, to ensure that:**

8.2.1 the customer or end user is aware that his personal information is transferred outside the borders of the RSA, or to a third party, for the sole and exclusive purpose of performing the duties as set out in the agreement between the Alarm company and the customer;

8.2.2 the third party cloud server host is subject to a binding law or binding personal information processing policy or binding agreement which provide adequate protection against personal information processing;

8.2.3 the transfer of data is for the sole benefit of the customer or end user.

8.3 The Communication service provider must supply the Alarm company with its and/or the third party host's best practice policy for the safe and secure transferring of personal information processing.

8.4 The Communication service provider must immediately inform the Alarm company if and when a breach has occurred in the secure transferring of personal information together with the details of such breach as required in terms of the POPI Act.

## 9. Repeater sites

9.1 The equipment must be housed in a secure, stable enclosed structure.

9.2 It is recommended that access doors be metal doors with an enclosed locking mechanism or additional security gate.

9.3 It is recommended that windows and ventilation ducts are secured with a high security grid of no less than 5mm steel bars.

9.4 An effective ventilation is required to keep the equipment within a safe operating temperature not exceeding 40 degrees celsius.

9.5 Backup power system to be capable of supporting the repeater equipment for a minimum period of 24 hours. Backup power may consist of auto start fuel generator, wind generator, solar power or AC charged battery bank.

9.6 Equipment to be installed, allowing open space between equipment for adequate ventilation and ease of access. Equipment racks are recommended.

9.7 Where easy access to the antenna cable carrier frame between the mast and building is possible, enclosed metal carrier frames are recommended.

9.8 It is recommended that Access to the repeater equipment enclosure or structure to be monitored via available communication method where possible.

9.9 The structure must be fitted with a fire extinguisher for electrical fires.

9.10 Where safe access is possible, 24 hour access should be available for technical staff.

## 10. Local Servers

10.1 Local servers must have a backup mirrored server.

10.2 Server and data communication equipment to be installed in a lockable server rack within the control room or in a secure server room.

10.3 Alternate technology internet access fail over connection is required such as, fibre to LTE, Wireless WAN or SAT internet.

10.4 A dedicated backup power system is required for the server rack, its receivers and data communication equipment.

10.5 Backup power to the server must sustain the entire communication system for a minimum of 24 hours.