COMMUNICATION TECHNOLOGIES FOR INTRUDER ALARM MONITORING

SAIDSA®

1. Communication methods

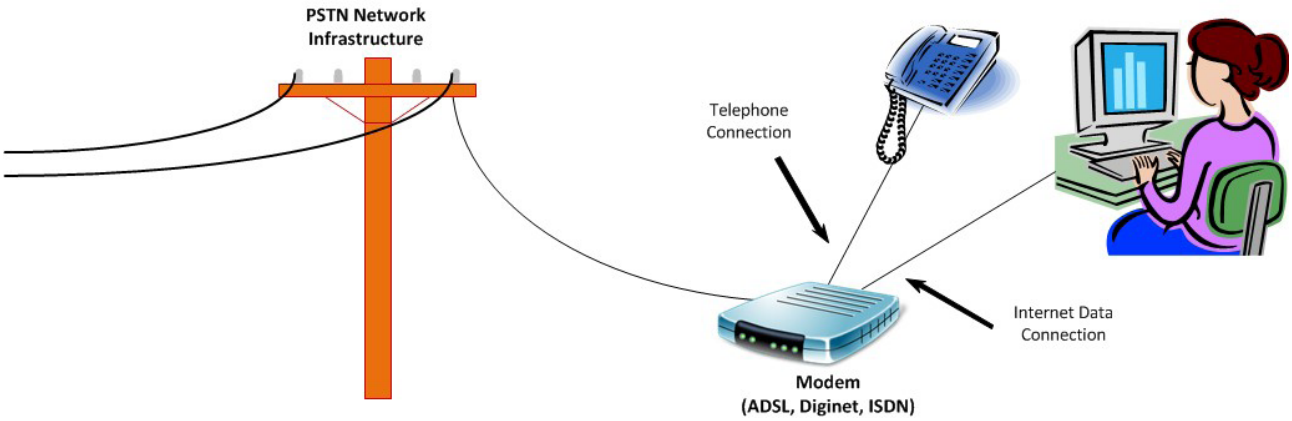
There are only two Last-mile options available to connect a residence or building's security system to a central monitoring station and these are Landline (Buried & Overhead cables) and Wireless (Via the air, no physical connection)

It is not uncommon for a Central Control Room service provider to make use of a combination of Landlines and Wireless technologies, to create a network infrastructure which communicates signals from a multitude of locations back to their Central Control Room in order to provide redundancy within their networks.

Land line

Land line refers to the multitude of Copper or Optical fibre cables installed, between buildings and the local Post Office Exchange, which was initially intended for analogue Telephone lines. The monitoring of alarm signals via telephone phone lines has been the worldwide industry standard since the mid- 1980s. The PSTN (Public Switched Telephone Network) was initially a network of fixed-line analogue telephone systems consisting of a pair of copper wires that ran from a residences or business back to the Local Exchange in different areas. Local Exchanges was cabled back to a Metropolitan Exchange and so on. Since then technologies have significantly improved with the evolution of the Internet.

Today, only the older parts of the PSTN utilize analogue technology whereas most new telecommunications Exchanges utilizes digital systems. Advances in digital communications and the increased use of fibre optic cable as a replacement of copper wire has greatly improved communication speeds and available bandwidth.



Wireless

Wireless refers to multiple technologies commonly known as RF, Microwave, Satellite, WiFi, DSSS and GSM that uses radio waves to transmit and receive signals via the air.
In South Africa the monitoring of alarm systems by using high power RF (Radio Frequency) transmitters was introduced in the early 1990's. The concept was based on telemetry monitoring method used by Eskom and Rand Water who made use of 2-way high power radios to monitor and control the flow of electricity and water remotely. The introduction of cellular phones technology that uses the GSM (Global System for Mobile communications) infrastructure, has taken the wireless approach to a whole new dimensions. GSM technology added the ability to monitor and control security systems remotely via Voice, SMS and the Internet.

In the alarm monitoring industry there are various wireless technologies throughout the HF, VHF and UHF frequency bands available.

Wireless technologies can be split into two infrastructural categories which are as follows:

Private
This category groups 1-way and 2-way RF radio transmission (low and high power) networks together that relies on a private network infrastructure. This infrastructure covers geographical areas which are serviced by Individual Network Providers, Remote CCTV and Alarm monitoring companies. These RF networks make use of licensed frequencies owned by Individual Network Providers or alarm monitoring companies.

Public
This category includes all types of communication networks that make use of RF technology to provide communications infrastructures for the general public, such as GSM, DSSS and includes dedicated 1-way and 2-way RF radio networks utilizing public access frequencies.

2. Alarm communicator interfacing methods

For alarm monitoring, there are a large variety of communicators available. These communicators act as an interface between the alarm system and the communication network used by remote monitoring companies.

There are three different interfaces used to connect the Alarm systems to communicators, which are as follows:

2.1 POTS (Plain Old Telephone System)
Most alarm systems come with an onboard POTS communicator to facilitate reporting of events via PSTN networks. Theses communicators predominately make use of DTMF (Dual-Tone Multi Frequency) signaling to communicate events. The communication format stemmed from the Telephone keypad which consist of 16 different keys (0 to 9, *, # plus four function) each with its own DTMF tone.

2.2 Comms Port (Communications Port)
Some alarm systems have dedicated serial communication ports for the transport of data. The most common is the Keybus, which refers to the communications termination of ancillary devices such as keypads and expanders. Some system comes with a secondary port for 3rd party integration like an RS-232 port.

2.3 I/O (Input and Output)
This is the lowest level of interfacing as event information is limited to the interpretation of the relative I/O status change.

3. Central station communications options

For the Security market there are essentially only four different communication paths available namely PSTN, VHF RF, DSSS and GSM. Each of these paths offers various methods of communication.

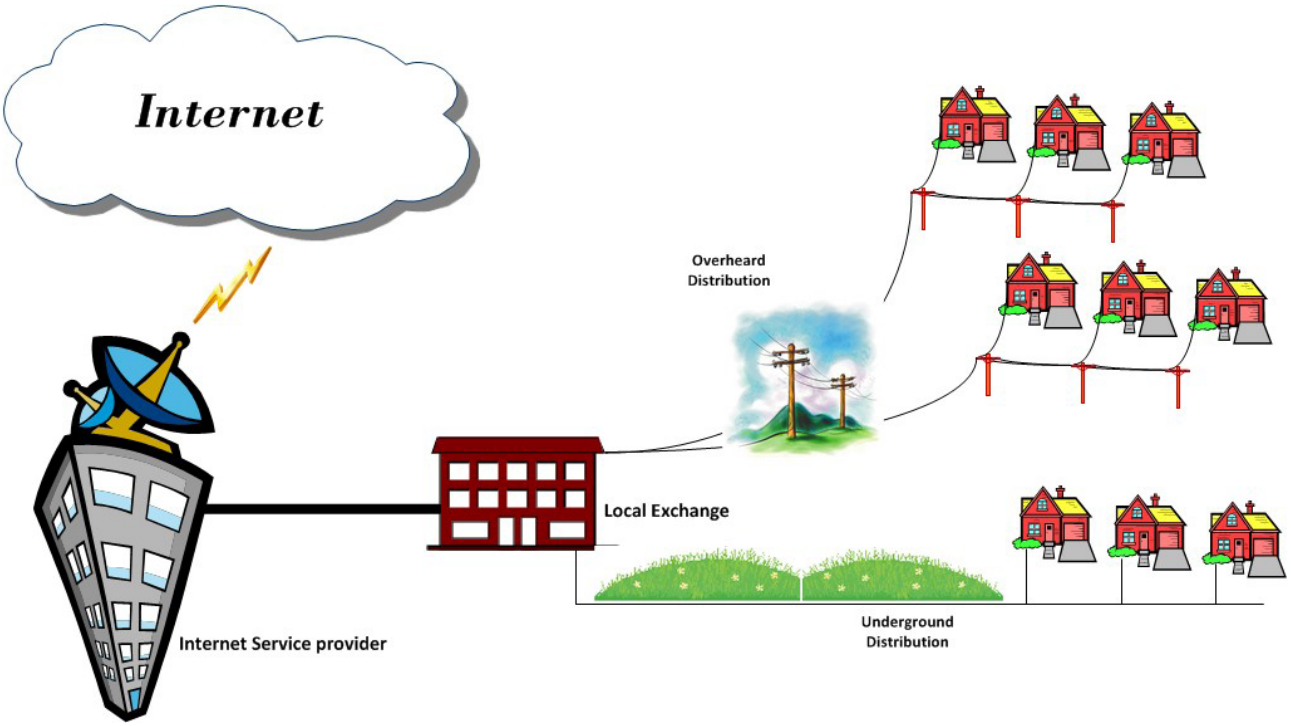
3.1 PSTN (Public Switched Telephone Network)
This consists of a copper or fibre cable between premises and the local Post Office Exchange, initially intended for public telephone network use. The move from analogue to digital exchange systems created a platform that went from voice only to voice and high speed data transmission formats.

PSTN is short for ***Public Switched Telephone Network***, and refers to the international telephone system, based on copper wires carrying analogue voice data. Newer technologies such as ***ISDN (Integrated Services Digital Network)*** and ***VoIP (Voice over Internet Protocol)*** are more commonly found, especially in the commercial industry where multiple simultaneous connections are required. A telephone service using the PSTN infrastructure is often

called plain old telephone service (POTS).

Most alarm systems come with an onboard PSTN communicator. There are over 70 different PSTN proprietary protocols from different alarm system manufactures using either a Digital Data Modem or DTMF modem technology to communicate alarm events through to a central station. Initially Central Stations required a dedicated PSTN Base Station ***(Receiver)*** for every protocol used. On demand of Central Stations, multiprotocol receivers were developed and Alarm System manufacturer's then followed suit with Alarm systems supporting their own proprietary plus one or two of the more commonly used protocols.

In 1999 ***SIA (Security Industry Association)*** published the DC-05 document based on the ***"Ademco Contact ID"*** alarm communication format with the sole purpose for Alarm manufacturer's to adopt this format in order to ensure across- the-board compatibility.
Commonly known as either ***Contact ID*** or ***Point ID***, because of its resilience against bad quality PSTN lines, has become an industry norm as an alternative (to propriety) protocol supported by Alarm systems. Contact ID uses DTMF modem technology to communicate alarm events through to Central Stations.



Communication sequence - When an alarm occurs, the control panel seizes the phone line and dials the Monitoring station. At the Monitoring station a PSTN Base Station picks up the call and begins to send a sequence of ***"Handshakes"*** each identifying a particular communications protocol.

If the PSTN Base Station is able to translate the sequence, it will send a ***"Kiss-off"*** signal to indicate to the control panel that it understood the signal. The Base Station will then wait for a few seconds giving the control panel the opportunity to send another event. If no additional events are communicated by the control panel within the waiting period the Base Station will disconnect from the PSTN line, and wait for the next call.

Communication Methods

- **Voice (via POTS)** – Refers to the voice channel available for a PSTN connection. Most alarm systems come with an onboard modem to facilitate full bidirectional communication.

- **TCP/IP (via DSL, ADSL & DIGINET)** – Refers to the digital channel of a PSTN connection. TCP/IP communicators are either onboard or part of the ancillary modules

of security system and provide for full bidirectional communication. When used in conjunction with PSTN it forms part of the Internet infrastructure.

PTSN Summary

- Relies on public network infrastructure;
- Allows for bidirectional communication;
- Allows for acknowledgement of receipt between alarm panel and control centre;
- Full event information utilizing the correct interface;
- Nationally established
- Cable root could be open to sabotage
- PTSN communication is susceptible to lightning

3.2 IP (Internet Protocol)

IP is short for Internet Protocol and refers to a communication method used to send and receive data via the Internet. The Internet is a name for ***"interconnection of computer networks"*** via a public network infrastructure, which globally connects millions of personal, business and governmental computers together enabling them to intercommunicate.

The Internet was initially developed using the then existing PSTN infrastructure as a bidirectional digital, point to point, relayed communication medium, commonly known as a Dialup connection between ***ISPs (Internet Service Providers)*** and the rest of the world. With the introduction of ISDN, ADSL and Diginet modems ***(PSTN interfaces)*** the need for actual PSTN Data modems to first establish a Dialup connection to the Internet is no longer required. Furthermore, as digital technology improved, advances were made in the amount of data throughput between connection points, better known as ***Bandwidth*** today.

Today connection to the Internet is predominately established either by means of public ***PSTN (using ISDN, ADSL and Diginet modems)*** or via the public Cellular ***(using GPRS and 3G Routers or Modems)*** network infrastructures. As an alternative or backup connection, corporations use Bidirectional Microwave links between them and ISPs to provide a redundancy Internet connection.

Intrusion

IP interfaces for alarm system are predominately add-on modules which connect to the alarm system's Control Panel by means of PSTN, Comms Port or I/Os terminations. Generally these interfaces make use of propriety protocols, meaning that Central Stations would require an IP Receiver ***(Base Station)*** from the same manufacturer to interpret the alarm event information for the Central Station's ***EMS (Event Management System)*** to use.

Bandwidth Consideration:

Bandwidth utilization to send an event via IP is minuscule as the information contains not much more than a Panel identifier, Zone number, Zone Type, Zone Status and associate Partition number in the event of an alarm. Even with a few additional bits for ***CRC (Circle Redundancy Check)*** the amount of information is less than what is required for a basic connection handshake between two computers over the Internet.

3.3 CCTV (Closed Circuit Television)

With CCTV systems the IP interfaces generally forms part of the on-site control equipment such as the DVR, NVR or Management Computer. As with Alarm systems CCTV manufacturers prefer using propriety communication formats to send and receive data via IP, ensuring their own ***VMS (Video Managements Systems)*** or client applications are used.

Through the years many attempts were made to introduce a common communication format, based on the demands from the industry. In 2008, CCTV equipment manufacturer's Axis Communications, Bosch Security Systems and Sony formed an organization called ***ONVIF (Open Network Video Interface Forum)*** with the goal to create an international standard for IP products within the video surveillance industry in order to ensure across-the-board compatibility.

Bandwidth Consideration:
Bandwidth utilization is an important consideration when required to monitor a CCTV system remotely via IP. The factors include the number of simultaneous cameras being viewed, the image resolution used, the compression type and ratio, frame rates as well as scene complexity. This has to be put into context with the Internet connection method being used like ISDN, ADSL and Diginet as each have its own upload limitation controlled by ether the technology or relative ISP.

Typical South African Internet Connection methods reflecting maximum available Up/Download speeds are as follows:

Technology	Upload speed	Download speed
ISDN	128Kbps	128Kbps
Diginet	512Kbps	512Kbps
1Meg ADSL	128kbps	1Mbps
2Meg ADSL	256kbps	2Mbps
4Meg ADSL	512kbps	4Mbps

ADSL maximum bandwidth is based on best service principle as the available bandwidth could be shared with up to 20 other subscribers. Although GSM/Data like 3G is also an Internet connection option it is not recommend. The cost implication to stream video images for long periods of time would be exorbitant.

In order to make bandwidth utilization more predictive IP CCTV equipment manufacturers have introduced a configuration setting within the video compression settings to limit/control bandwidth utilization of relative video streams. This setting is based on two basic concepts as follows:

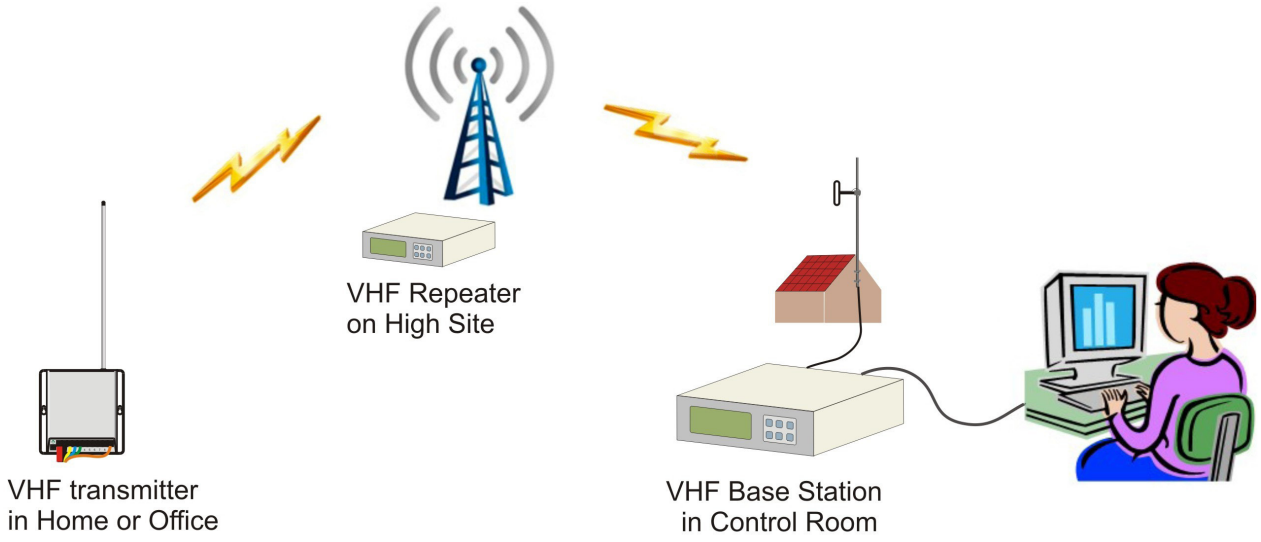
- **Variable Bit Rate** – VBR encoding method allows the user to specify a bit rate range — a minimum and/or maximum allowed bit rate. Some encoders extend this method with an average bit rate. With this option image quality prevails.
- **Constant Bit Rate** – CBR encoding method allows the user to specify a fixed bit rate at which the CODEC has to output the video stream, irrespective of changes in the scene. Within this option image quality is sacrificed should the scene become complex based on changes or movement within the scene.

Irrespective of the choice made the maximum bit rate selected multiplied by the amount of simultaneous video streams to be viewed remotely plus the maximum bit rate times by the amount of video streams being recorded remotely equates to the IP connection's bandwidth requirement. This requirement should be taken in consideration when selecting an Internet connection method.

3.4 RF transmitters

This is the use of single ***(simplex)*** Radio Frequencies ***(RF)*** to communicate signals on a Point to Point basis or to a relayed RF network infrastructure via radio transmitters.
The transmitters make use of ***Frequency Modulation (FM)*** to transfer the information being sent. Multiple transmitters transmit signals to the same receiver station or base station. The transmitted signal can feed into an RF network of repeaters that will communicate signals back to a central monitoring station over the allowed distance stipulated in the allocated ICASA licence.
These radio transmitters use either licenced or non licenced frequencies and interfaces to a security system by means of PSTN, Serial port or individual inputs.

Communication Methods:
VHF and UHF, – Refers to single carrier frequency radio transmitters which transmit alarm signals to a receiver. The transmitters make use of ***Frequency Modulation (FM)*** to transfer the information being sent. Multiple transmitters transmit signals to the same receiver station. The transmitted signal can feed into an RF network of repeaters that will communicate signals back to a central monitoring station over the allowed distance stipulated in the allocated ICASA licence.
RF (Radio frequency) transmitters are mainly divided in to three groups namely VHF, UHF and Microwave.



3.4.1 VHF - (Very High Frequency)

Long range transmitters are used to communicate on a radio frequency allocated by ICASA and are licenced for distances up to a 50 km radius. 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 or PSTN . Once the VHF signal is received by the repeater, it is linked into a GPRS or PTSN modem that communicates with the central monitoring station where it is received by a GPRS or PTSN 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.

3.4.2 UHF – (Ultra High Frequency)

Short range transmissions are provided on license free frequencies for short hop communications ranging from a few to several hundred metres. Short range transmitters do not require a license from ICASA, however they are restricted to very low RF output power and to specific shared and sometimes congested frequency allocations. Typically the short range transmitter will be used to provide secondary equipment link communications to other primary communications equipment which will transfer the information over a longer distance. The primary equipment may include any of the other communication systems described in this document.

RF Antennae:

Antenna's used are the indoor ***folded dipole*** or ***whip.*** The whip antenna is more commonly used as it is inexpensive and easier to install. The whip antenna's length is determined by the operating frequency and therefore can mostly only be used on the frequency supplied.
The folded dipole is expensive and bulky to mount. It is however matched to the whole operating frequency band and therefore can be used on any channel within the allocated frequency band.

3.4.3 Microwave

Refers to Point-to-Point RF communication links (1 or 2-Way) that make use of frequencies available in the Microwave band 2.4 to 5 GHz. Microwave links employ multiple modulation techniques depending on the application used. A frequency licence is required from ICASA. Microwave is mostly used for video monitoring links that can report movement or intrusion detection.

Microwave Antennae:

Microwave directional dish antennas for correct frequency band.

RF Transmitter Summary:

- Does not rely on public network infrastructure
- Does not allow for bidirectional communication
- Does not allow for acknowledgement of receipt between alarm panel and control centre
- Capable of full event information reporting
- Nationally available on application
- Not easily sabotaged
- RF communication is not susceptible to lightning

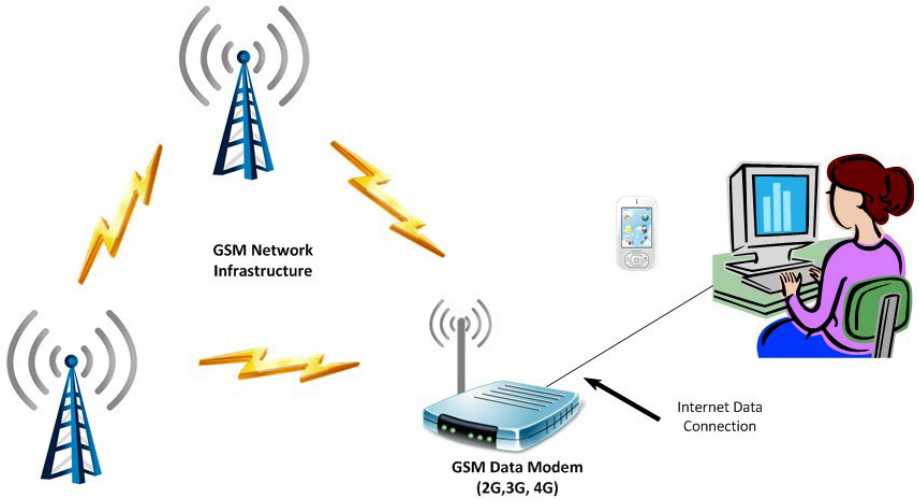
In addition to the above, the following points have reference to RF technology:

- Requires an ICASA control room frequency registration
- Ownership of VHF frequencies by Alarm Monitoring Companies is possible.
- Operating area is network dependant and mostly limited to 50km radius area.
- Simplex frequencies have limited transmitter load capacity.
- Companies with frequency ownership must establish their own repeater networks.

3.5 GSM

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 and 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 individual inputs, 4x1, 4x1 extended, 4x2, Ademco Point ID, Contact ID, and SIA.



3.5.1 GPRS and SMS

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.

Antennae

Quad band on-board or screw-on whip antennas are used. Magnetic mount whip antennas are available with various cable lengths to allow extended positioning the antenna to obtain a

better signal connection to the GSM network.

3.5.2 GSM Data

The GSM network is a public infrastructure, initially developed for Mobile phone applications. With advances in this Digital RF technology other forms of communication methods were incorporated into the GSM services.

A ***Data Transceiver (DT)*** always communicates through an ***Access Point Name (APN)*** on the GSM network. The APN is responsible for authenticating a DT onto the GSM network and relay information between a DT and its destination *(typically a server or IP enabled device)*. Most DT's are provisioned on a private APN which provides a dedicated communications channel without having to share bandwidth with users on the public APN. There are however instances where a DT is provisioned on the public APN, either as the primary means of communication or as a backup method. DT's communicate with the ***Internet Protocol (IP)*** and may use any protocol ***(TCP, UDP, FTP, etc.)*** on the transport layer. In most cases a proprietary protocol with encryption is communicated on the application layer. Information communicated on DT networks is not human interpretable like with SVT's and therefore requires a translation device such as a base station and/or computer application to translate the information.
DT networks in the security industry are typically made up of a server which is responsible for relaying messages between two or more DT's *(A transceiver and a base station)*.

In simple terms, a DT network is made up of two or more DT's and a relay server with one or more DT's being installed at the monitoring site/s and another DT *(a base station)* at the control room which will output its signals to a computer running monitoring software, interpreting the signals from the DT. Usually the customer is not involved with the complexities of the network and server.

Even though a DT is primarily used to communicate data, some DT's have added functionality to communicate via SMS and voice. SMS is typically used as a backup method should a DT network fail or to receive control commands via SMS and voice *(missed call)*. To overcome the problem with a failing DT network, redundancy is introduced by using dual SIM, dual APN's and in some cases dual servers.

Communication Methods

- **Voice** – Refers to communicators that simulate PSTN connection via the GSM network. These communicators utilise the voice channel of the GSM network to communicate to the PSTN lines at the central control rooms.

- **SMS** – Refers to communicators that utilize the ***SMS (Short Message System)*** channel of the GSM network to connect to the SMS receiver at the central control rooms.

- **Data** – Refers to communicators that utilize the Data channel of the GSM network and allow for TCP/IP communication via the Internet.

GSM Transceiver Summary:

- Relies on public network infrastructure
- Allows for bidirectional communication
- Allows for acknowledgement of receipt between GPRS transceiver and control centre
- Full event information utilizing the correct interface
- Nationally established
- Can be sabotaged with commercially available jamming equipment
- RF communication not susceptible to lightning

3.6 DSSS

DSSS-(Direct Sequence Spread Spectrum) alarm data communication was established in South Africa and has been operating since 2006, building and expanding its networks. The network has currently been tailor designed to suite the alarm security industry and offers full bi-directional communications for signal acknowledgement and anti-jamming technology.

The current network coverage as to 2014, is the greater Gauteng and the greater Cape Town

area, and plans are in place to expand the network to Durban, Bloemfontein and other metropolitan areas. The DSSS technology uses a packet scheduled means of data transmission and reception that is highly immune to jamming and interference. The DSSS is a propriety dedicated network allowing only DSSS transceivers to operate on its network.

DSSS is a *radio frequency (RF)* communication system in which the baseband signal bandwidth is intentionally spread over a large bandwidth by injecting a high-frequency signal.
Thus energy used in transmitting the signal is spread over a wide bandwidth, and appears as noise. Due to the spread spectrum technology it penetrates through difficult areas and urban noise. It does not use repeater sites but rather relies on the small scheduled packages of data with low RF power to be amplified by the receivers, either synchronously or asynchronously, with multiple acknowledgement stages. The fact that the data is scheduled and transmission and reception of data packages is managed, the loss of signals are basically zero.

DSSS transceiver summary:

- The transmission of data takes place in a scheduled network, so it is not susceptible to collisions and congestion i.e. loss of signals.
- Relies on the public network infrastructure by choice
- Allows for bidirectional communication
- Allows for acknowledgement of receipt between DSSS transceiver and control centre
- Full event information utilizing the correct interface
- Not nationally established
- Not easily sabotaged
- RF Communication are not susceptible to lightning

Antennae
Screw-on band matched PCB whip antenna.

4. Central Station Communication Implementation and Infrastructure

4.1 PSTN

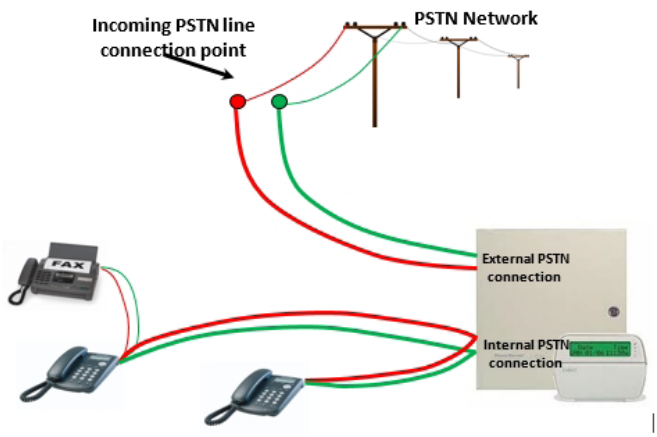
Installation of communications devices
As most alarm systems come with an onboard PSTN communicator, other than programming the control panel's with the relative parameters such as phone numbers, preferred communication protocol and which event types need to be communicated, all that is required is to connect the control panel to the Phone Line connection point.

It is important to note that the control panels must be wired to the PSTN line in such a way that it would be able to seize the phone line where the line is being shared with other devises such as Telephone handsets and/or FAX machines.

PSTN connection to Alarm systems

Control room installation requirements
Sufficient quantity of PSTN lines to cope with quantity of alarm panels to be monitored without losing alarm events.

Base station requirements
Sufficient quantity of PSTN base stations (Receivers) compatible with alarm protocols used by alarm system required to be monitored.



PSTN connection to alarm systems

4.2 IP

Interfacing to IP network infrastructure (LAN)

Connecting of an IP communicator to a customer's LAN (Local Area Network) should be done in collaboration with the customer's network specialist.
The physical termination between IP communicator and LAN is relatively easy. All it takes is to connect the one end network Patch cord to the communicator and the other end to a mating LAN wall socket. However the IP communicator needs to be programmed to function correctly on the relative LAN as well as report alarm events to the relative Central Station's.

Base station requirements

Sufficient quantity of IP base stations (receivers) compatible with IP communicators used by alarm system required to be monitored.

4.3 CCTV

The physical connection of a CCTV system, or an IP Camera, to a customer's network infrastructure for remote monitoring purposes requires no additional interfaces. The relative interfaces are built-in to the system's control equipment such as a DVR, NVR or Management PC/ Server.

Installation of communications devices

As with Intrusion systems, connecting of a CCTV system's control equipment (in the case of a total IP solution including cameras) to a customer's Internet enabled network infrastructure should be done in collaboration with the customer's network specialist.

The physical termination between the customer's network and the CCTV system's control equipment is relatively easy. All it takes is to connect the one end network patch cord to the system's control device and the other end to a LAN connection point. However the control equipment needs to be programmed to function correctly on the relative LAN as well as being accessible to facilitate remote control and viewing from the relevant central stations.

Control room installation requirements

Compatible remote video management system or client software

Base Station Requirements

No Base station required

4.4 VHF/UHF

Installation of communications devices

A VHF transmitter operates on the 12V DC alarm supply backup battery. Connection to the transmitter from the alarm panel is via individual trigger, serial port or CID PTSN connection. The DC supply cable to the transmitter must be at least 0.5mm wire connected directly to the battery terminals and not exceeding 6 metres. The transmitter with a whip antenna (or dipole) must be vertically mounted and not near metal objects, cable or electronic devices including the alarm PIR detectors and keypads as the RF power can affect their operation.

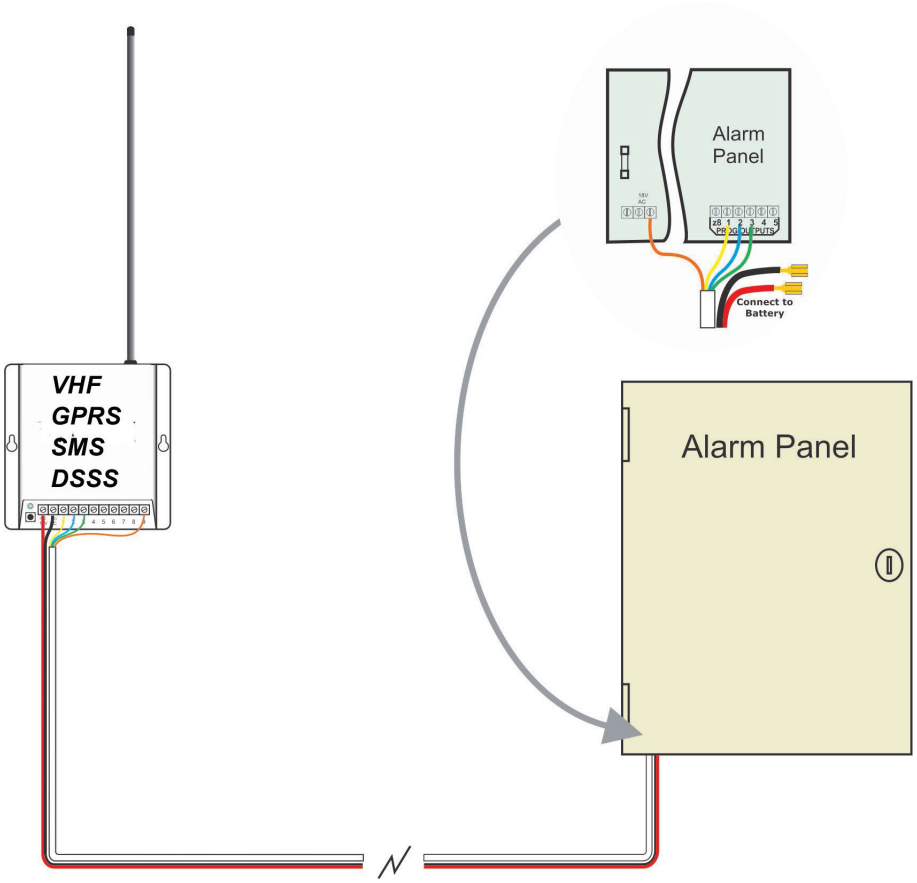
VHF transmitter connection to alarm systems

Control room installation requirements

VHF receiver equipment should be enclosed in a communications tower *(19 inch lockable rack)* or a purpose built communication room. Adequate space, cooling and lighting must be provided in the communication tower / room. This will provide adequate room for maintenance and keep the equipment within safe operating temperatures.

Base station requirements.

Adequate receivers must be available to handle the monitored transmitter load. Backup equipment must be kept with the operational receiver and programmed for direct replacement if required.



Connection to alarm systems

Hi-Sites / Repeaters
Repeater sites must be secure, protected from the elements and monitored for intrusion or equipment tampering. Access to the site at all hours is crucial for maintenance.

4.5 GPRS, SMS

Installation of communications devices
A GPRS/SMS transceiver operates on the 12V DC alarm supply backup battery. Connection to the transceiver from the alarm panel is via individual trigger, serial port or CID PTSN connection.
It is important to use 0.5mm cable for the DC supply and to connect directly to the battery terminals.
The unit must be placed away from the alarm panel and peripheral devices, where its signal strength will be at an optimal signal level.

Control room installation requirements
The GPRS/SMS base must have an adequate antenna that will provide an uninterrupted connection to the GSM network. Dual network paths can be used for additional network integrity.

4.6 DSSS

Installation of communications devices
A DSSS radio transceiver operates on the 12V DC alarm supply backup battery. Connection to the transceiver from the alarm panel is via individual trigger, serial port or CID PTSN connection.
It is important to use at least 0.25mm cable for the DC supply and to connect directly to the battery terminals. On installation the transceiver position can be determined by using the onboard 8 segment signal strength display to obtain the best link to the network.

Control room installation requirements

Access of signals are through the web/internet and service provider VPN.

There are different combination means of getting connectivity into DSSS provider VPN, to date they are:

1. Telkom Diginet line failing over to Fastnet
2. ADSL line failing over to Fastnet
3. I Burst and VSAT

Base station requirements

No base station required.

5. ICASA

REGULATORY COMPLIANCE WITH THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA (ICASA)

ICASA's mandate is explained in the Electronic Communications Act for the licensing and regulation of electronic communications and broadcasting services, and by the Postal Services Act for the regulation of the postal sector

Enabling legislation also empowers ICASA to monitor licensee compliance with license terms and conditions, develop regulations for the three sectors, plan and manage the radio frequency spectrum as well as protect consumers of these services.

Functions of ICASA

- ☐ To license broadcasters, signal distributors, providers of telecommunication services and postal services
- ☐ To make regulations
- ☐ To impose license conditions
- ☐ To plan, assign, control, enforce and manage the frequency spectrum
- ☐ To ensure international and regional co-operation
- ☐ To ensure interoperability of networks;
- ☐ To receive and resolve complaints

Herewith follows frequently asked questions:

- **Who needs a radio frequency spectrum licence?**
- Any South African registered entity that intends using the radio frequency spectrum must apply for the Licence.
- ***Broadly, what are the document requirements for an application for radio frequency spectrum licence?***
- A stamped commissioner of oath completed radio frequency spectrum application form.
- Entity's registration document
- Payment of the requisite fee
- Submission of anticipated coverage polygon for the calculation of the exact licence fee

- ***Is the radio frequency spectrum licencing a once off payment?***
- No, the licence has to be renewed annually at a cost.
- ***What is type approval?***
- Type Approval is a process by which communications equipment / device or system are authorised by the Authority (ICASA) to be used in South Africa which will involve verification of the item's compliance with the applicable standards and other regulatory requirements. All alarm monitoring transmitter or transceiver products must be type approved by ICASA.
- ***What is the purpose of the ICASA Label on equipment.***
- All type approved equipment need to be properly labeled with ICASA type approval sticker bearing the authority's logo and the type approval number of the device.
- ***What is a Radio dealer certificate***

- Any Business entity that intends storing and selling radio communications items at its premises must obtain a radio dealer certificate
- The process for acquiring the certificate includes filling in an application form, submission of the entity's registration details including business address and the required application fee needs to be paid.
- The licence is renewable annually.
  It is important to note that all licences have conditions that licensees need to adhere to and failure to comply with the conditions specified may result in penalties being imposed on the licence holder. It is therefore crucial that the licensees familiarise themselves with applicable licensing conditions for their respective licences they hold to avoid fines.

NOTE: The communication methods described in this document are of the most popular found in the South African Security Industry. Variations of these technologies may also be avaiable.