GSM Interceptor System

Technical Parameter

Model: P4-X

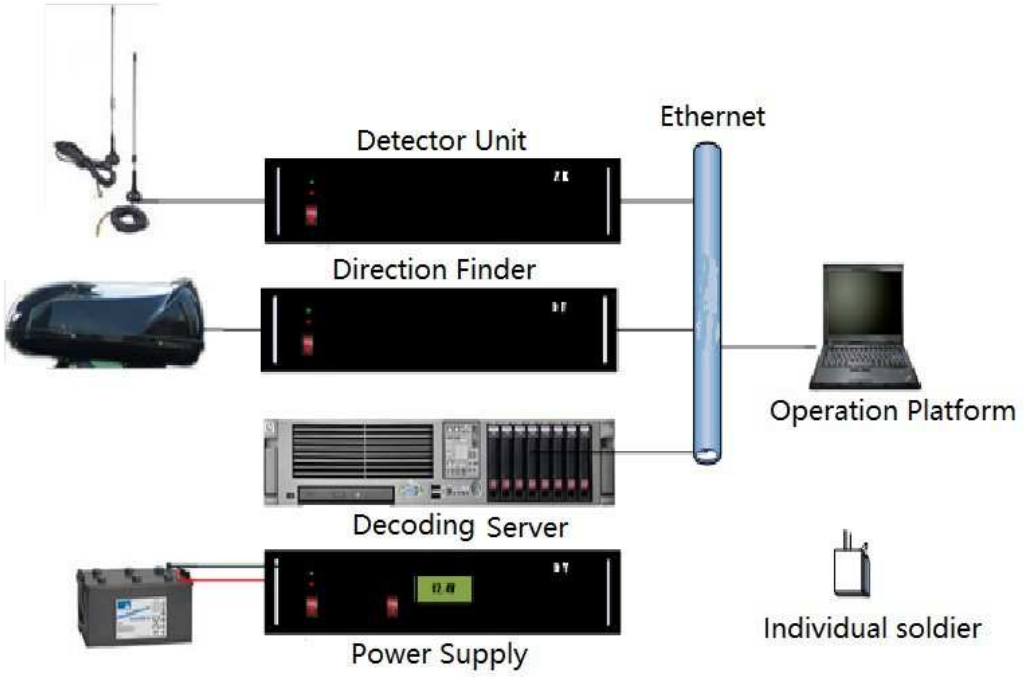


Table of Contents

1 Introduction 7
2 References 7
3 Abbreviations 7
4 System Overview 8
4.1 Introduction of the Wind Catcher System 8
4.2 Technical Advantages and Features of Functions 9
4.3 Main Functions of the Wind Catcher System 13
4.4 Technical Specifications of the Wind Catcher System 13
4.5 System Composition 14
5 Technical Specifications of the Vehicle Subsystem 16
5.1 Objective 16
5.2 Composition of the Vehicle Subsystem 17
5.2.1 Hardware Structure of the Vehicle Subsystem 17
5.2.2 Monitoring Unit 17
5.2.3 Decryption &Processing Unit 17
5.2.4 Direction Finding Unit 18
5.2.5 Multi-Point Assisted Positioning Unit 18
5.2.6 Operation & Maintenance Unit 18
5.2.7 Vehicle Power Supply Unit 18
5.2.8 Equipment list of the Vehicle Subsystem 18
5.3 Technical Parameters and Requirements of the Vehicle Subsystem 19
5.3.1 Main Functions of the Vehicle Subsystem 19
5.3.2 Technical Specifications of the Vehicle Subsystem 20
6 Fixed Station Subsystem 21
6.1 Objective 21
6.2 Composition of the Fixed station Subsystem 21
6.2.1 Hardware Structure of the Fixed Station Subsystem 21
6.2.2 Monitoring Unit 22
6.2.3 Decryption &Processing Unit 22
6.2.4 Operation &Maintenance Work Station 23

6.2.5 UPS Power Supply Unit 23
6.2.6 Equipment Composition of the Fixed Station Subsystem 23
6.3 Technical Specifications and Requirements of the Fixed Station Subsystem 24
6.3.1 Main Functions of the Fixed Station Subsystem 24
6.4 Technical Specifications of the Fixed Station Subsystem 25
7 Technical Specifications of the Individual-Soldier Subsystem 25
7.1 Objective 25
7.2 Composition of the Individual-Soldier Subsystem 25
7.2.1 Hardware Structure of the Individual-Soldier Subsystem 25
7.2.2 Individual-Soldier Side 26
7.2.3 Composition of the Individual-Soldier Subsystem 26
7.3 Technical Parameters and Requirements 27
7.3.1 Main Functions of the Individual-Soldier Subsystem 27
7.3.2 Technical Specifications of the Individual-Soldier Subsystem 27
8 Detailed Description of the Vehicle Subsystem's Functions 27
8.1 Management of Monitoring Equipment 27
8.1.1 Checking of Versions of Monitoring Unit's Hardware and Software 27
8.1.2 Turning on and off of Monitoring Unit 27
8.1.3 Checking of Monitoring Unit's Equipment Status 28
8.1.4 Task Operations on the Monitoring Unit 28
8.2 Management of Triggering Device 28
8.2.1 Checking Status of the Triggering Device 28
8.2.2 Simulation of Mobile Phone 29
8.3 Management of Direction Finding Device 29
8.3.1 Checking of Version Information of the Direction Finding Device 29
8.3.2 Checking of Status of the Direction Finding Device 29
8.3.3 Start and Stop of the Direction Finding Device 29
8.3.4 Parameter Management of the Direction Finding Device 30
8.3.5 Calibration and Examination of the Direction Finding Device 30
8.4 Scanning of Cell Information 30
8.4.1 Scanning of Full Frequency Information 30
8.4.2 Scanning of the Appointed Operator's Information 30

8.4.3 Scanning of Information of the Appointed Frequencies 31
8.4.4 BER Testing 31
8.5 Management of Local Information 31
8.5.1 Output of Monitoring Module's Information 31
8.5.2 Deletion and Storage of Local Information 31
8.6 Management of Network Information 31
8.6.1 Output of Monitoring Modules' Network Information 31
8.6.2 Deletion and Storage of Network Information 32
8.7 Management of Random Interception 32
8.7.1 Task Management of Random Interception 32
8.7.2 Real-Time/Quasi-Real-Time Decryption of the Random Interception 32
8.7.3 Voice Monitoring by the Random Interception 32
8.7.4 Automatic Storage and Management of Voice 32
8.7.5 SMS Interception by the Random Interception Function 33
8.7.6 Automatic Storage and Browsing of SMS Function 33
8.8 Management of Specific Target Interception 34
8.8.1 Management of Specific Target Interception 34
8.8.2 Real-Time/Quasi-Real-Time Decryption of Specific Target Task 34
8.8.3 Manual Capturing of Specific Target 34
8.8.4 Automatic Capturing of Specific Target 34
8.8.5 Monitoring of Specific Target's Voice 35
8.8.6 Automatic Storage and Management of Specific Target's Voice 35
8.8.7 Interception of Specific Target' SMS 35
8.8.8 Automatic Storage and Browsing of Specific Target's SMS 36
8.8.9 Direction Finding (DF) of Specific Target 36
8.8.10 Processing and Recording of Specific Target's DF Results 36
8.8.11 Sending of Specific Target's DF Results to the Front-End Screen 36
8.8.12 Display of Current Location on GIS Map 36
8.8.13 Adding of DF Results on the GIS Map and Assisted Positioning 37
9 Detailed Description of Functions of the Fixed Station Subsystem 37
9.1 Management of Monitoring Devices 37
9.1.1 Checking of Versions of Monitoring Unit's Hardware and Software 37

9.1.2 Turning on and off of Monitoring Unit 38
9.1.3 Checking Status of the Monitoring Unit 38
9.1.4 Task Operations on Monitoring Unit 38
9.2 Management of Triggering Device 39
9.2.1 Checking Status of the Triggering Device 39
9.2.2 Simulation of Mobile Phone by the Triggering Device 39
9.3 Cell Information Scanning 39
9.3.1 Scanning Information on Full Frequency 39
9.3.2 Scanning Information of an Appointed Operator 40
9.3.3 Scanning Information of the Appointed Frequencies 40
9.3.4 BER Testing 41
9.4 Local Information Management 41
9.4.1 Output of Information from Monitoring Modules 41
9.4.2 Deletion and Storage of Local Information 41
9.5 Management of Network Information 41
9.5.1 Output of Monitoring Modules' Network Information 41
9.5.2 Deletion and Storage of Network Information 41
9.6 Management of Random Interception 42
9.6.1 Task Management of Random Interception 42
9.6.2 Real-Time/Quasi-Real-Time Decryption of the Random Interception 42
9.6.3 Voice Monitoring by the Random Interception 42
9.6.4 Automatic Storage and Management of Voice 42
9.6.5 SMS Interception by the Random Interception Function 43
9.6.6 Automatic Storage and Browsing of SMS Monitored 43
9.7 Management of Specific Target Interception 43
9.7.1 Management of Specific Target Interception 43
9.7.2 Real-Time/Quasi-Real-Time Decryption of Specific Target Task 44
9.7.3 Manual Capturing of Specific Target 44
9.7.4 Automatic Capturing of Specific Target 44
9.7.5 Monitoring of Specific Target's Voice 45
9.7.6 Automatic Storage and Management of Specific Target's Voice 45
9.7.7 Interception of Specific Target' SMS 45

9.7.8 Automatic Storage and Browsing of Specific Target's SMS 46

10 Detailed Description of Individual-Soldier Subsystem's Functions..... 46

10.1 Turning on and off of Transmission Device of Individual-Soldier Subsystem (On the Vehicle Side) 46

10.2 Turning on and off of Individual-Soldier Subsystem (Individual-Soldier Side) 46

10.3 Connection of Bluetooth Transceiver on the Individual Soldier Side 46

10.4 Communication between Individual Soldier Subsystem and the Vehicle Subsystem.. 47

10.5 Determination of Target's Direction by Values in Triggering SMS..... 47

1 Introduction

The General Technical Specifications contains the technical specifications for Wind Catcher System, which specify the equipment composition, main technical parameters and requirements, requirements for package, transportation and storage, etc. of Wind Catcher System.

2 References

Clauses for technical parameters of Wind Catcher System are specified in the appendix of the Contract.

3 Abbreviations

GSM	*Global System for Mobile communications*
A5/1	*Encryption algorithm A5/1*
A5/2	*Encryption algorithm A5/2*
AGCH	*Access Grant CHannel*
FCCH	*Frequency Correction CHannel*
MSISDN	*Mobile Station Integrated Services Digital Number*
IMSI	*International Mobile Subscriber Identity*
TMSI	*Temporary Mobile Subscriber Identity*
IMEI	*International Mobile Equipment Identity*
LAC	*Location Area Code*
CI	*Cell Identity*
GPS	*Global Positioning System*
GIS	*Georgraphic Information System*
TDOA	*Time Difference Of Arrival*

E-OTD	*Enhanced-Observed Time Difference*
FAT	*Factory Acceptance Test*
SAT	*Site Acceptance Test*
WiFi	*Wireless Fidelity*

4 System Overview

4.1 Introduction of the Wind Catcher System

The Wind Catcher System adopts the well-developed passive multi-channel phase-comparison method and antenna array to acquire the air signaling information and traffic information of base station and users from the GSM wireless interface. It can detect the target when which is stand-by, and conducts precise direction-finding and positioning through several points. Once the target is on the phone, the surveillance and positioning is immediately initiated.

Moving at a speed of 60 km/h, the Wind Catcher System can still locate the GSM mobile phone target in a city or under other complicated conditions, and implement high-precision (accuracy: ±1°) direction finding and positioning. It is still hard for the target to run away, even if he accelerates drastically (e.g.100km/h), because the system will keep tracking and positioning.

This system is available in three formats: vehicle subsystem, fixed station subsystem and individual-soldier subsystem.

The vehicle subsystem adopts a 5-channel parallel phase-comparison technique, to accomplish one direction finding every 5μS (positioning accuracy: ±1°). Multi-channel intercepts on line at the same time; its design can easily do brick-pattern stacking.

In addition, the system is equipped with GPS and a gyro-assisted location system, which can automatically scan a vehicle system and locate the target by using multi-point intersections, as well as conduct long-distance locating and high-speed tracking on targets.

The fixed station subsystem is designed to meet needs of long-period uninterrupted real-time interception at a specific area. With a high-gain receiving antenna to increase gain of long-distance signals, the system can increase interception distance with prerequisite of good voice quality.

The individual-soldier subsystem is small in size and easy to disguise. It connects to the vehicle subsystem through WiFi and implements location to a house, person, or even the specific position of a mobile phone. A Bluetooth connection is used inside the system, which can be easily concealed.

4.2 Technical Advantages and Features of Functions

1. *The system has the following technical advantages comparing with the other interception-positioning systems at the interception aspect:*

Table-1 **technical advantage at interception aspect**

Item	Other randomly interception systems	Wind Catcher System
Decryption	*Slow: they need at least 1 minute to decrypt A51 algorithms*	*Accurate: high decryption rate* *Fast: supports real-time decryption of A52 algorithms and quasi-real-time decryption of A51 algorithms.*
Surveillance scope	*Small: They can only monitor a fixed number of cells at the same time. At the same cost, they monitor fewer cells. Small surveillance scope.*	*Large: It can monitor a flexible number of cells. At the same cost, it monitors more cells. Large surveillance scope.*
Frequency point monitoring mode	*Restricted: They monitor the same frequency point at all channels. Low capture ratio. If the target cell is not in the Cells under Surveillance Table, they can't switch to the target cell to continue trace.*	*Unrestricted: It does not monitor channels at a fixed frequency point, but tracks dynamically. High capture ratio. If the target cell's signal is good enough to be received, it can switch to the cell and continue trace.*
Direction-finding tracing speed	*Slow: They can't find direction by the first SMS trigger; Switch among LA tracing areas is slow; TMSI changes slowly.*	*Fast: It can finds direction by the first SMS triggering; Switch among LAC areas is fast; TMSI changes fast.*

Cell monitoring mode	*Fixed: They allocate a fixed number of modules to each of the cells under surveillance without consideration of imbalanced traffic distribution in cells. Low capture ratio.*	*Flexible: It allocates modules to cells under surveillance dynamically with consideration of various traffic distribution conditions in cells. High capture ratio.*

2、 The system has the following technical advantages comparing with the other interception-positioning systems at the direction-finding aspect:

Table-2 Technical advantages at the direction-finding aspect

Amplitude-comparison direction finding and positioning system	**Wind Catcher System 5-channel parallel correlative interferometer.**
Imprecise: It shows results in vectors and should be located near to the target. The process lasts long, easy to be known by targets.	*Precise: It shows results in linear way and can locate a target from long-distance. The process lasts short, and not easy to be found by targets.*
Slow: User should change angle of antenna or change antennas themselves for many times to get a direction finding result; trigger targets for many times in one direction finding. Low speed; easy to be exposed.	*Fast: User do not need to change angle or change antennas and get a direction finding result from one signal sampling handle; over 10 direction finding results can be obtained by single trigger; high speed; not easy to be exposed.*
Weak: It estimates direction only by amplitude and is sensitive to interference; bad anti-interference performance; low precision.	*Strong: It comprehensively uses phase and amplitude and is not sensitive to additive interference; good anti-interference performance; high precision.*

3、Comprehensive Technical Advantages

1) Real-time/quasi-real-time decryption of A5.1/A5/2

The Wind Catcher System provides the most advanced and best real-time decryption equipment for A5.1 and A5.2 algorithms, to ensure effect of interception of real-time voice and SMS.

2) Passive 3rd party wireless interception—large coverage, no-interference, flexible

The System is only used as a communication connection between the passive receiving base station and mobile phones, and does not need to confront and suppress signals from telecommunication operators' base stations, so it does not transmit signals. Accordingly, it does not interfere and produce radiation to operators' base stations, surrounding mobile phones, and operators of the system. And it is of low power consumption.

As a passive system as long as it can receive signals from a base station, it could find the target. Accordingly, comparing with active systems, it has a large working range with up to 20 kilometers interception distance between itself and a target in actual case solving.

Active systems can only find direction with IMEI and could not obtain conversation and SMS contents, while this system can intercept and position a target only with its phone number, and could obtain voice communication and SMS contents.

3) Multi-module, dynamic targeted-signal tracing technology

A typical configuration of this system uses 10 independent signal receiving channels (interception modules) to trace air signals dynamically. The interception modules could be configured and used dynamically according to operating parameters of the GSM network, repeated coverage environment of the base stations, and air communication traffic conditions in the target environment. Theoretically, the system can trace maximum 10 cells at the same time. It greatly enhanced adaptability of the system to the GSM network environment: it adopts a variable TMSI/IMSI mobile phone identification mode and controls information encryption mode, which realizes high efficient and fast capture and trace of the target air signal, and low air signal missing probability at low cost.

4) Correlative interferometer direction finding system—accurate, adoption of a fixed antenna array

The vehicle subsystem is a direction finding unit designed with an advanced 5-channel parallel correlative interferometer phase-comparison direction finding technique. The traditional amplitude-comparison direction finding method uses a directional antenna, and determines electric wave direction by the maximum (minimum) amplitude of a signal received. The traditional system is easy to be realized but is with low sensitivity, bad accuracy, and bad interference-suppression performance. The direction finding technique used by our system adopts phase-comparison mechanism, which uses a fixed (no need to be turned)

omnidirectional antenna array and determines direction of a coming electric wave by processing signals and analyzing vector signals constituted by the phase and amplitude of it, besides, it has a large interception-control range and is of high precision (the traditional amplitude-comparison mechanism shows results in sector way, while this system show in liner way) and less influenced by the network. And, the advanced correlative interferometer in this mechanism eliminates as greatly as possible the interference on direction finding results, such as reflection from metal articles like cars. Because the estimation of direction finding result is showed in a liner method, so this system can use a multi-point assisted positioning technique. Besides, the small omnidirectional antenna array (including protection cover) is only ø500×100mm, which is helpful to equipment modification and disguise.

5) 5-channel parallel correlative direction finding processing –precise and fast

Based on the correlative interferometer phase-comparison mechanism, with consideration of discontinuity of GSM signals and its burst short pulse transmission, we designed the 5-channel parallel acquisition and processing system with high technology content. By this system, end users do not need to turn off and on or change antennas in a direction finding. It accomplishes one precise direction finding every 5μS and 100 high-reliable directions finding in 0.55μS cycle of one GSM burst. Thus, it increased speed, and ensures reliability and high precision of direction finding in a fast changing environment. We got a ±1°direction finding in calibration measure.

6) Modular structure—easy to expand, install and apply

The system adopts a modular structure, is small in size and easy to expand, install, disguise, and can be installed on various types of vehicles. Currently, an off-road vehicle is recommended because of its high environmental adaptability. It adopts a low-consumption power supply which can be charged by vehicle battery to meet normal needs.

To sum up, main features of the Wind Catcher System can be concluded as follows:

No.	System Feature	Advantage of the feature
1	*Passive 3rd party wireless interception*	*Large coverage, no interference, flexible*
2	*Correlative interferometer direction finding system*	*Precise, with a fixed antenna array;*
3	*5-channel parallel correlative direction finding processing*	*Precise and fast*

4	*Fast + passive wireless interception and positioning*	*Good adaptability to telecommunication networks;*
5	*Signal processing system based*	*Advanced technology, good performance, small in size, and low power consumption;*
6	*Modular structure*	*Easy to expand, install and apply*

4.3 Main Functions of the Wind Catcher System

- *The system monitors air signal environment in the network, including operator identities, LAC, CI, configuration of the frequency point, and signal intensity, etc.*
- *The system can intercept a specific target, namely, it traces and monitors calls and SMS of a specific phone number or of a specific incoming or outgoing phone number.*
- *It can also intercept a whole access process from start a call to control and allocation, and obtain parameters such as voice, SMS, incoming and outgoing phone numbers, and TMSI/IMSI, etc.*
- *The system is able to check air voice information and monitor voice already in a communication.*
- *The system can locate a targeted phone, i.e. it conducts a fast wireless direction finding of a targeted phone in the above mentioned interception processes; Or just with a phone number, no matter TMSI or TMSI is adopted by the network, the system can trace the target's TMSI/IMSI parameter codes by related parameters interception, matching, and acquisition in the air to conduct direction finding fast.*
- *It supports interception and positioning in systems adopting A51/52 encryption measures and A50 systems without encryption.*

4.4 Technical Specifications of the Wind Catcher System

Main Technical Specifications of the Wind Catcher System:

- *Supports 900/1800MHz dual-frequency GSM networks, no need to reconfigure the system for this*

- *Supports non-hopping/hopping networks*
- *Supports variable/ invariable IMSI, TMSI operation modes and encrypted network*
- *Supports various network operating parameters and switches, no need to reconfigure the system.*
- *Configurable channel quantity of interception system.*
- *Supports real-time decryption of A52 encryption systems (lab testing environment)*

  Decryption rate: *100%*

  Decryption speed: *0.05～1s*

- *Supports quasi-real-time decryption of A51 encryption systems (lab testing environment):*

  Decryption rate: *>70%*

  Decryption speed: *3～5s*

- *Receiver sensitivity:* *-100～-103dBm*
- *Direction finding estimate speed:* *<0.5ms/time*
- *Direction finding estimate precision (by calibration measurement)*

  ±1°
- *Antenna size(including protective cover):* *ø500×100mm*
- *Power supply of the system:* *< 220V、0.6*Ａ
- *Environmental temperature:* *0*℃～*50*℃
- *Environmental humidity:* *15%～85%*

4.5 System Composition

The whole system consists of "vehicle subsystem, fixed station subsystem, and individual-soldier subsystem". The following section will specify them in detail.

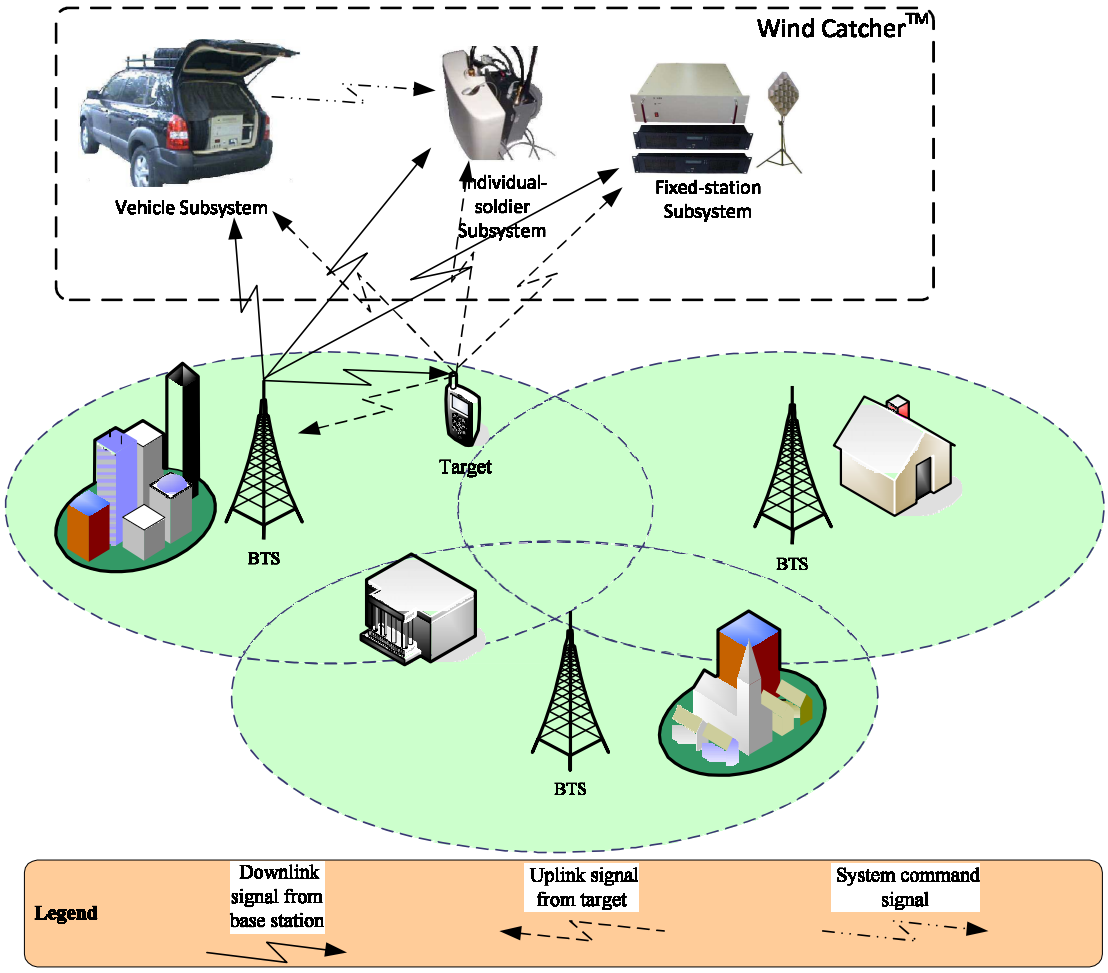


Figure-1 Composition of the Wind Catcher System

1. Vehicle subsystem

The monitoring unit of the vehicle subsystem mainly receives and processes downlink and uplink voice and signaling at Um interface. It consists of main monitoring unit and monitoring antenna. The main monitoring unit is comprised by uplink and downlink receiving channels whose quantity can be configured flexibly, and each of which receives one line of uplink and downlink access.

The decryption unit processes decryption of signaling received by the monitoring unit, recovering signaling encrypted.

Assisted by the monitoring unit, the vehicle direction finding unit calculates direction of the target and is comprised by the main direction finding main unit and the 5-channle antenna array. The vehicle direction finding unit receives data from the uplink radio signal at channels given by the monitoring unit calculates and gets reliable direction information.

The multi-point assisted positioning unit conducts CAD drawing according to a lot of direction information calculated on many spots, assisted with a computer. It helps the equipment operators to determine the most reliable direction of the target. It is comprised by a GPS receiver and a gyro.

2. Individual-soldier subsystem

The individual-soldier subsystem is used to approach and locate the target when he is near to the operator. It is comprised by the individual-soldier receiving module, transmission channel, and directional antenna, etc.

3. Fixed station subsystem

The fixed station subsystem is designed to meet needs of long-period uninterrupted real-time interception at a specific area. With a high-gain receiving antenna to increase gain of long-distance signals, based on optimal fixed-station monitoring unit, the system can increase interception distance with prerequisite of good voice quality.

According to different needs of interception of uplink and downlink signals, directional and omnidirectional antenna suites are provided.

The monitoring unit of the vehicle subsystem is mainly used to receive and process downlink and uplink voice and signaling from Um interface. It consists of main monitoring unit and monitoring antenna. The main monitoring unit is comprised by uplink and downlink receiving channels of which the quantity can be configured flexibly, and each of which receives one line of uplink and downlink access.

The decryption unit processes decryption of signaling received by the monitoring unit and recovers signaling encrypted.

5 Technical Specifications of the Vehicle Subsystem

5.1 Objective

This section mainly describes the system structure, composition, equipment list, main functions, and technical specifications of the vehicle subsystem.

5.2 Composition of the Vehicle Subsystem

5.2.1 Hardware Structure of the Vehicle Subsystem

The vehicle subsystem consists of monitoring unit, A51/A52 processing unit, direction-finding unit, and multi-point assisted positioning unit, operation and maintenance unit and vehicle power supply unit. Please see details in the following figure:

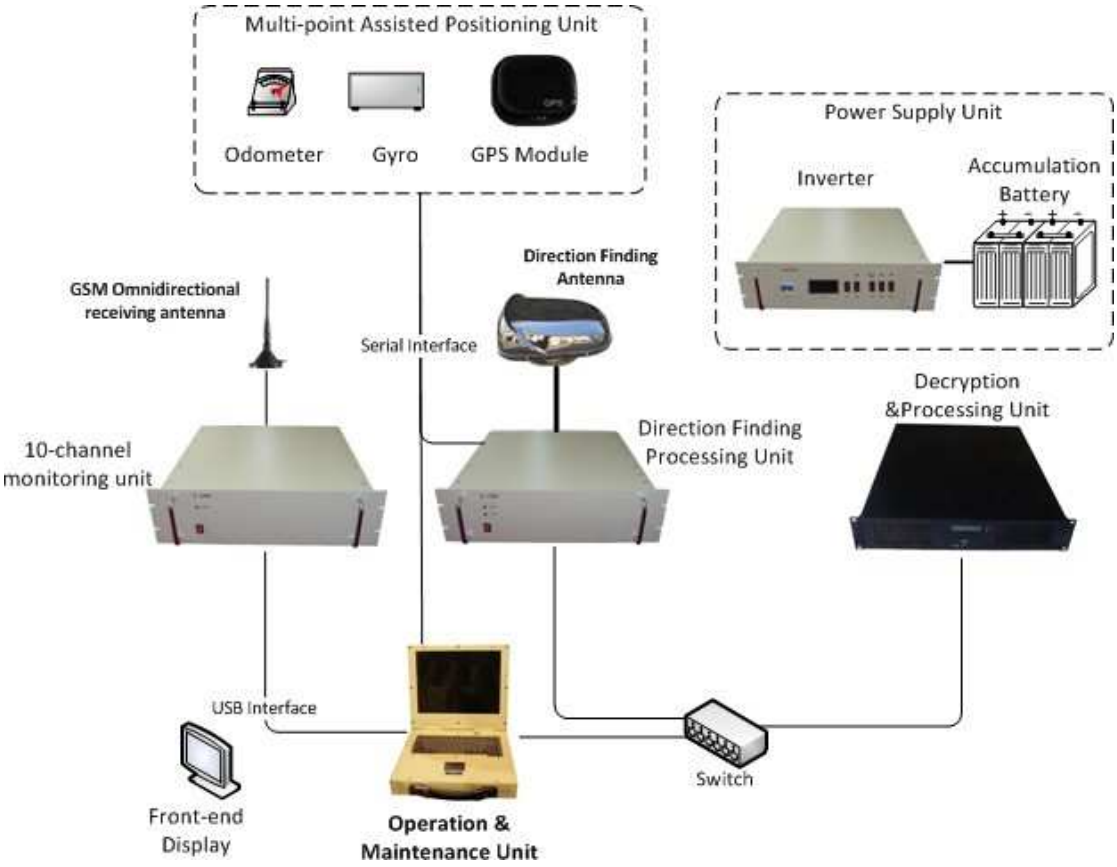


Figure-2 Vehicle Subsystem Composition

5.2.2 Monitoring Unit

The monitoring unit receives and processes the uplink and downlink voice and signaling from Um interface. The monitoring unit consists of main monitoring unit and monitoring antenna. The main monitoring unit includes the uplink and downlink channels (each channel can receive one uplink and downlink access) whose quantity can be flexibly configured.

5.2.3 Decryption &Processing Unit

The decryption &processing unit receives encrypted frame data from Um interface

forwarded by the monitoring unit, decrypts those encrypted data, and obtains Kc parameters within required time so as to recover original signaling data, SMS and voice data by the monitoring unit, etc.

5.2.4 Direction Finding Unit

Cooperated by the monitoring unit, the vehicle direction finding unit calculates the target's direction. It consists of main direction finding unit and a 5-channel antenna array. The vehicle direction finding unit receives data from the uplink radio signals on channels provided by the monitoring unit, after calculation processing, provides reliable direction information.

5.2.5 Multi-Point Assisted Positioning Unit

By multiple direction information measured on many points, the multi-point assisted positioning unit conducts CAD (computer assisted drafting) drawing to assist operators in determination of a reliable target direction. The multi-point assisted unit consists of a GPS receiver and a gyro.

5.2.6 Operation & Maintenance Unit

The operation &maintenance unit consists of a control platform and a front-end display. It is used to allocate tasks to the above-mentioned units, set parameters, display results, manage and maintenance those units, and import, display electronic map and GPS location information, and is the display interface of multi-point positioning unit. The hardware of the control platform is an military standard portable laptop, and the software is a Win32 application program operating on Windows XP operating system. The front-end display is used to show direction finding results for vehicle driver to decide vehicle route.

5.2.7 Vehicle Power Supply Unit

The vehicle power supply unit provides power supply to the other units in the vehicle subsystem. It consists of a storage battery pack, inverter etc. The storage battery pack is charged by the vehicle engine, after inverted by from DC to AC, provides corresponding level of AC power to the other units.

5.2.8 Equipment list of the Vehicle Subsystem

Table-3 Equipment list of the Vehicle Subsystem

No.	Functional Component	Quantity
1	*10-channel 900/1800MHz dual-frequency parallel receiving and interception unit*	**1set**

2	*High-gain 900/1800MHz receiving antenna and feeder*	**1 suit**
3	*5-channeldigital/parallel/correlative/fast/high-precision/direction-finding processor*	**1 set**
4	*5-unit direction finding array antenna*	**1 set**
5	*Signal feeder and controlling feeder exclusive for direction finding use*	**1 suit**
6	*System controlling military standard laptop*	**1 set**
7	*PCMCIA plug-in card for target triggering device*	**1 set**
8	*Hub*	**1 set**
9	*System equipment drive and control software, etc*	**1 suit**
10	*Engineering model mobile phone exclusive for network monitoring use*	**1 set**
11	*High-precision vehicle e-gyro*	**1 set**
12	*GPS receiver*	**1 set**
13	*GIS control and data processing software*	**1suit**
14	*Decryption &processing unit*	**1 suit**
15	**Vehicle power supply unit**	**1 suit**

5.3 Technical Parameters and Requirements of the Vehicle Subsystem

5.3.1 Main Functions of the Vehicle Subsystem

- *The vehicle subsystem monitors air signal environment of the network, including the operator's identity, LAC, CI, frequency point configuration, signal intensity, etc.*
- *The vehicle subsystem monitors air voice information and voice of phones being in communication.*
- *It intercepts the whole connection process of a call, besides voice information it can obtain incoming phone number, etc.*
- *Concealed SMS triggers target secretly.*
- *It can intercept a specific target; it can trace and intercept calls of a specific phone number or a specific incoming phone number.*
- *It can position a targeted mobile phone. In the above mentioned interception processes, it can conduct a fast wireless direction-finding positioning to the targeted mobile phone in communication; Or just with*

the phone number of the target mobile, whether the network is under TMSI or IMSI operation mode, the vehicle subsystem can position it by the target's TMSI, IMSI parameters obtained by interception of network system parameters in the air.

- *It can fast precisely locate a fixed or moving mobile phone from a long or near distance.*
- *Third-party wireless interception--- large coverage, no-interference, flexible*
- *It sends a transparent SMS to the target mobile phone to trigger it without known by the target subscriber.*
- *Auto storage of voice and SMS intercepted, and stores complete relative interception information including: phone numbers of the calling and called party, time, contents, etc. Besides, the system is able to playback, add, and delete voice and SMS intercepted.*

5.3.2 Technical Specifications of the Vehicle Subsystem

- *The vehicle subsystem automatically supports 900/1800MHz dual frequency working mode*
- *Automatic supports hopping frequency /non-hopping frequency working modes*
- *Supports variable and invariable IMSI, TMSI network operation modes*
- *Supports various network operating parameters and switch working modes*
- *Maximum 20 pieces of system module can be configured*
- *System receiver sensitivity: -100～-103dBm*
  Direction finding speed: < 0.5ms
  Direction finding accuracy (calibration environment): ±1°
- *Antenna size (including protection cover) ø500×100mm*
- *System power supply: < 220V, 0.6*A
- *Environmental temperature: 0℃～50℃*
- *Environmental humidity: 15%～85%*

6 Fixed Station Subsystem

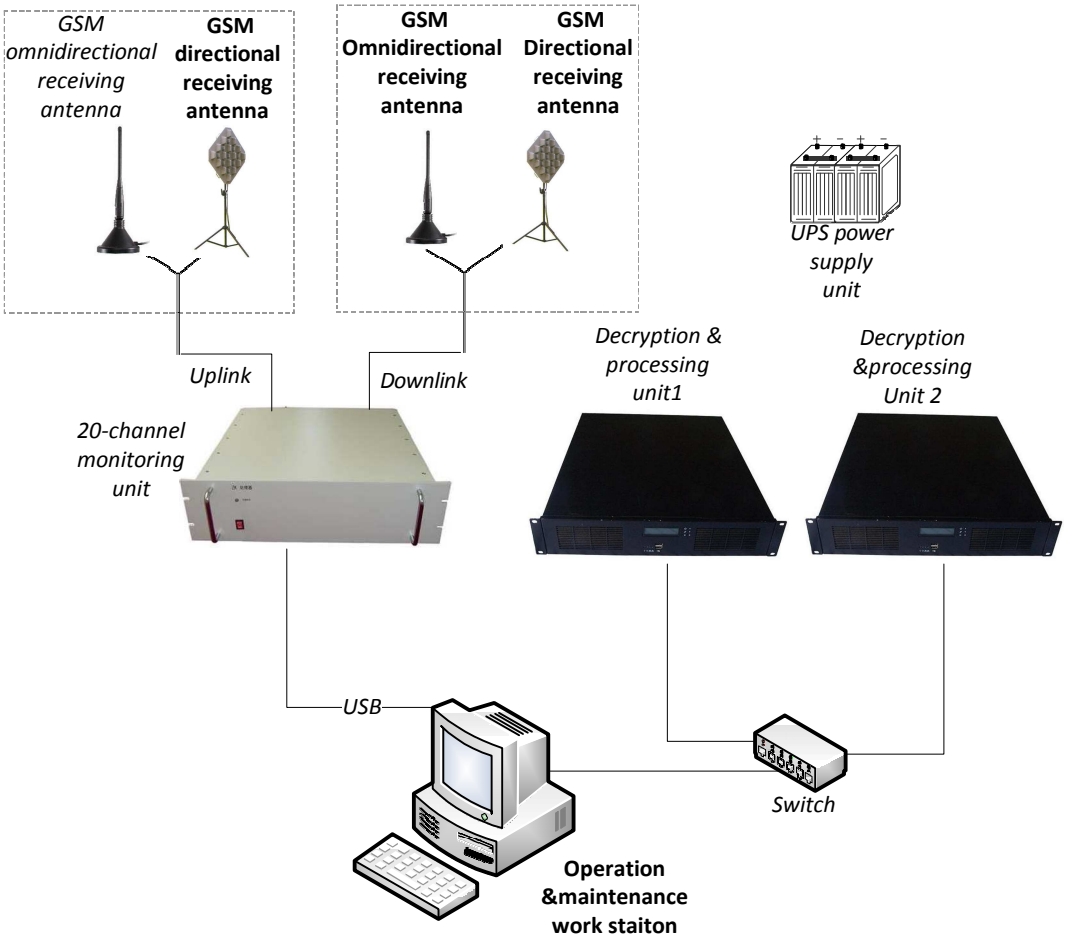
6.1 Objective

This section specifies the composition, equipment list, main functions and technical specifications of the fixed station subsystem.

6.2 Composition of the Fixed station Subsystem

6.2.1 Hardware Structure of the Fixed Station Subsystem

The fixed station subsystem is comprised by decryption &processing unit, monitoring unit, operation &maintenance work station and power supply unit. Please see structure of its full option configuration and of standard configuration in the following figures:



Talbe-3 Composition (full option) of the fixed station subsystem

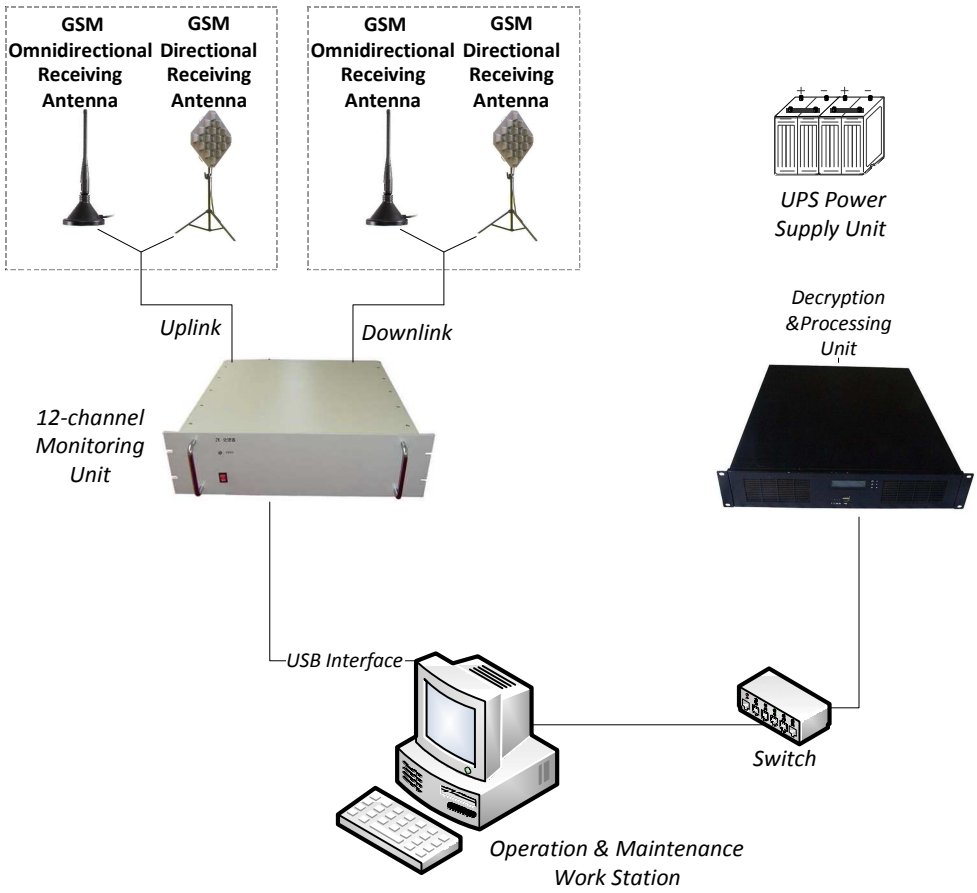


Figure-4 Composition (standard) of the fixed station subsystem

6.2.2 Monitoring Unit

The monitoring unit receives and processes uplink and downlink voice and signaling from Um interface. It is comprised by main monitoring unit and high-gain GSM receiving antenna. The performance and structure of this monitoring unit is optimized based on the monitoring unit of the vehicle subsystem.

The main monitoring unit is comprised by uplink and downlink receiving channels of which the quantity can be configured flexibly. Each channel can receive one line of uplink and downlink access; the GSM receiving antenna is provided in the format of directional antenna suite and omnidirectional antenna suite according to the needs of interception of uplink and downlink signals, which can respectively receive high-gain uplink and downlink GSM signals in a specific base station or at a specific area.

6.2.3 Decryption &Processing Unit

The decryption &processing unit receives encrypted frame data from air interface forwarded by the monitoring unit, and decrypt those data; compute Kc parameters

within required time so that the monitoring unit can recover signaling data, SMS data and voice data by it.

To ensure the effect of random interception, and increase the performance of concurrent interception of GSM voice traffic, 2 sets of decryption &processing unit are provided in the full option configuration.

6.2.4 Operation &Maintenance Work Station

The operation &maintenance work station is comprised of control platform (including target triggering equipment) which is used to allocate tasks to the above mentioned units, set parameters, display results, manage and maintain those units. To ensure the high concurrency of monitoring unit's random interception, the control platform should adopt high-performance work station as its hardware, while the software employs Win32 application program operating on Windows XP operating system. The target triggering equipment of the fixed station subsystem is used to intercept target voice and SMS in the vicinity of the location of the subsystem.

6.2.5 UPS Power Supply Unit

The UPS power supply unit powers all the units of the fixed station subsystem, including storage battery pack, inverter, etc. It charges the battery by the vehicle engine, and inverts electricity power in the storage battery into alternating current to provide correspondent levels of power to all the units in the vehicle subsystem.

6.2.6 Equipment Composition of the Fixed Station Subsystem

Talbe-4 Equipment list of the fixed station subsystem

NO.	Functional component	Quantity
1	*20-channel 900/1800MHz dual-frequency/parallel/receiving/monitoring unit*	*1 set*
2	*Dual-frequency omnidirectional/directional receiving antenna and feeder*	*2 suits*
3	*Decryption &processing unit*	*2 sets*
4	*Engineering model testing mobile phone*	*1 set*
5	*Operation &maintenance work station*	*1 set*
6	*16-interface LAN Switch*	*1 set*
7	*UPS power supply system (including storage battery)*	*1 suit*
8	*System equipment drive and control software,*	*1 suit*

	etc	
9	*PCMCIA plug-in card for target triggering*	*1 set*

Table-5 Equipment composition (standard) of the fixed station system

NO.	Functional component	Quantity
1	*12-channel 900/1800MHz dual-frequency parallel receiving monitoring unit*	*1 set*
2	*Dual-frequency/directional receiving antenna, feeder*	*2 suits*
3	*Decryption & processing unit*	*1 set*
4	*Engineering model testing mobile phone*	*1 set*
5	*Operation &processing work station*	*1 set*
6	*16-interface LAN Switch*	*1 set*
7	*UPS power supply system (including storage battery)*	*1 suit*
8	*System equipment drive and control software, etc*	*1 suit*
9	*PCMCIA plug-in card for target triggering*	*1 set*

6.3 Technical Specifications and Requirements of the Fixed Station Subsystem

6.3.1 Main Functions of the Fixed Station Subsystem

- *The fixed station subsystem monitors air signal environment of the network, including the operator's identity, LAC, CI, frequency point configuration, signal intensity, etc.*
- *The fixed station subsystem monitors air voice information and voice of phones being in communication; intercepts the whole connection process of a call, besides voice information it can obtain incoming phone number, etc; and monitors air voice information and voice of phones being in communication.*
- *It works in the GSM network environment encrypted by A51/A52 algorithms.*
- *It can trigger target by a concealed SMS.*

- *Auto storage of voice and SMS intercepted, and stores complete relative interception information including: phone numbers of the calling and called party, time, contents, etc. Besides, the system is able to playback, add, and delete voice and SMS intercepted.*

6.4 Technical Specifications of the Fixed Station Subsystem

- *The fixed station subsystem automatically supports 900/1800MHz dual frequency working mode*
- *Automatically supports hopping frequency /non-hopping frequency working modes*
- *Supports variable and invariable IMSI, TMSI network operation modes*
- *Supports various network operating parameters and switch working modes*
- *Decrypt and process signaling, voice and SMS encrypted by A51/A52 algorithms*
- *Receiver sensitivity: -100～-103dBm*
- *Quantity of system modules: 12～20 channels*

7 Technical Specifications of the Individual-Soldier Subsystem

7.1 Objective

This section describes the system composition, equipment list, main functions and technical specifications of the individual-soldier subsystem.

7.2 Composition of the Individual-Soldier Subsystem

7.2.1 Hardware Structure of the Individual-Soldier Subsystem

The individual-soldier direction finding subsystem consists of individual-soldier side (individual-soldier receiver, panel directional antenna, downlink receiving antenna, transmission and receiving antenna, Bluetooth audio converter and Bluetooth earphone) and internal individual-soldier side for the vehicle subsystem or the

portable subsystem(transmitting controller---installed in the interception host, and power amplifier). Please see details in the following figure:

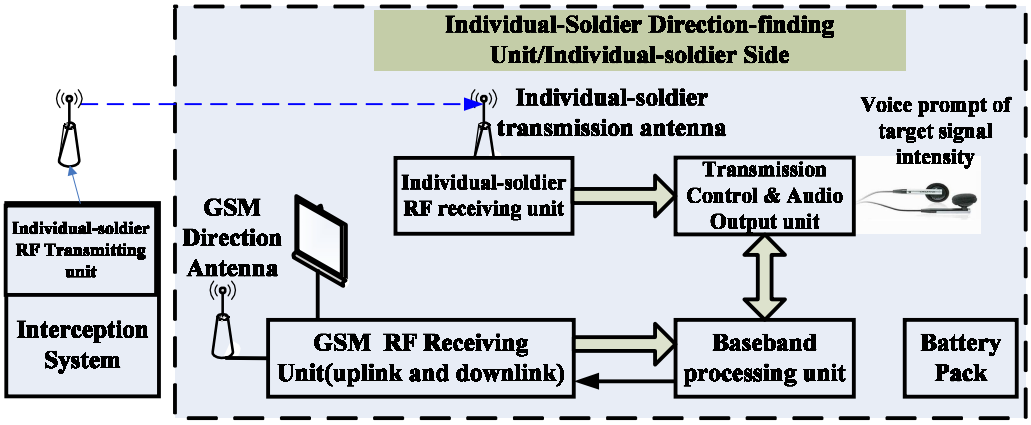


Figure-5 the composition block diagram of the individual-soldier subsystem

7.2.2 Individual-Soldier Side

In order to locate the target in a specific room or person, the system is equipped with the high-precision portable individual-soldier direction finding unit to realize the precision location of specific building, room, phone holder and phone position.

The working principle is to receive the target channel information transferred from monitoring unit by wireless transmission, measure the intensity of uplink signal, report the intensity results in voice form by Bluetooth earphone, combining the intensity report and directional antenna to judge the target location. The individual-soldier direction finding unit is small in size and weight, and portable. The direction finding result report will be prompted by voice, no need operator's extra operation. It is time saving and good concealment; besides, it frees operator's hands from operators for other tasks.

7.2.3 Composition of the Individual-Soldier Subsystem

Talbe-6 composition of the individual-soldier subsystem

No.	Functional Component	Qty
1	*Individual-soldier transmission equipment and antenna*	*1suit*
2	*Portable individual-soldier direction finding equipment (including communication receiving and direction finding machine)*	*2 suits*
3	*Battery and charger for individual-soldier*	*2 suits*

	subsystem	
4	*Individual-soldier controlling software*	*1suit*

7.3 Technical Parameters and Requirements

7.3.1 Main Functions of the Individual-Soldier Subsystem

Under control of the interception equipment the amplitude value of the target signal will be reported to individual-soldier subsystem operator in the form of voice value.

- *Amplitude value of the target signal will be reported in the form of voice.*
- *Wireless earphone connection to enhance the concealment function*
- *Use the amplitude-comparison directional antenna to judge the incoming direction of electric wave.*

7.3.2 Technical Specifications of the Individual-Soldier Subsystem

- *Directional antenna 3dB angle* ： *60°*
- *Distance between the wireless earphone and the individual-soldier equipment:* *about 3 meters*
- *Available battery time*： *6 hours*

8 Detailed Description of the Vehicle Subsystem's Functions

8.1 Management of Monitoring Equipment

8.1.1 Checking of Versions of Monitoring Unit's Hardware and Software

The system provides checking of serial numbers of monitoring modules in the monitoring unit, and version information of its hardware and software, including:

- *Serial numbers of monitoring modules*
- *Version Information of hardware*
- *Version information of software*

8.1.2 Turning on and off of Monitoring Unit

Users can turn on and off all the monitoring modules in the monitoring unit.

8.1.3 Checking of Monitoring Unit's Equipment Status

Users can browse the following information about monitoring modules in the monitoring unit in real time:

- *Turning off (by this time, all the interior information about modules is unknown)*
- *Idle (all the modules are ready to work, namely the status is ok)*
- *Status of Frequency scanning (when the status of modules are FCCH Scanning)*
- *Status of Signaling Tracking; by this time, the status of modules including:*
  - *WSYN: indicates that the module is synchronizing with the appointed frequency point;*
  - *AGCH: indicates that the module is monitoring network on certain frequency point;*
  - *SDCCH: indicates that the module follows some conversation on some frequency point and is entering into SDCCH channel*
  - *TCH: means that the module has already entered into some speech channel.*

8.1.4 Task Operations on the Monitoring Unit

According to requirements of tasks, the system provides monitoring modules with the following operations:

- *Start task*
- *Release task*
- *Restart task*

8.2 Management of Triggering Device

8.2.1 Checking Status of the Triggering Device

Users can browse the following status of the target triggering device which triggers the target covertly.

- *IMEI (identity) of the triggering device*
- *Name of the triggering device*
- *IMSI of the SIM card*
- *Current network signal Intensity on the triggering card*
- *Current status of the triggering card*
  - *Idle*
  - *Ringing or dialing*
- *The last missed call*
- *If new SMS is received*

8.2.2 Simulation of Mobile Phone

The triggering device can simulate mobile phone can conduct the following functions (different models of triggering devices may differ in functions):

- *Browsing received SMS*
- *Delete some or all received SMS*
- *Establish and send SMS*
- *Receive new SMS, and prompt the receiving*
- *Prompt of incoming call*
- *Receive or refuse a call*
- *Tuning of voice volume*

8.3 Management of Direction Finding Device

8.3.1 Checking of Version Information of the Direction Finding Device

Users can check version information of the direction finding device

8.3.2 Checking of Status of the Direction Finding Device

Users can check the current status of the direction finding device

8.3.3 Start and Stop of the Direction Finding Device

Users can start, stop and turn off the direction finding device

8.3.4 Parameter Management of the Direction Finding Device

Users can manage all the parameters for the direction finding device

8.3.5 Calibration and Examination of the Direction Finding Device

To ensure the accuracy of direction finding, the system provides calibration and self-examination to the direction finding device.

8.4 Scanning of Cell Information

8.4.1 Scanning of Full Frequency Information

The system provides scanning of all the frequency points on the GSM 900/1800MHz, the scanning results include;

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value，the unit is second*

8.4.2 Scanning of the Appointed Operator's Information

On both of the GSM900/1800MHz ranges, according to the customized operator, the system conducts frequency scanning to obtain all the following frequency information of the operator at the current location:

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value, the unit is second*

8.4.3 Scanning of Information of the Appointed Frequencies

On both of the GSM900/1800MHz ranges, the system provides information scanning of an appointed frequency point or band, the results include:

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value, the unit is second*

8.4.4 BER Testing

According to the frequency scanning results or an appointed frequency range, the system conduct BER testing to all the frequency points based on statistic time length, BER report cycle, and show the testing results on the frequency list.

8.5 Management of Local Information

8.5.1 Output of Monitoring Module's Information

By local information management, the system output operation and status information of all the monitoring modules, including: turning on of module, turning off of module, frequency scanning, task start, task implementation, etc.

8.5.2 Deletion and Storage of Local Information

The system provides functions of deletion and storage of local information.

8.6 Management of Network Information

8.6.1 Output of Monitoring Modules' Network Information

To the network information the system outputs various kinds of information about monitoring modules including:

- *Frequency monitoring information, namely frequency points the monitoring modules are monitoring;*

- *The network information are found: including TMSI, IMSI, calling ISDN number;*
- *Network synchronization information: synchronization and lost of synchronization with all the frequency points in the network;*
- *Network signaling information, including handover and hang-up.*
- *The information generates when the module enters into TCH and when follows target into cell handover.*

8.6.2 Deletion and Storage of Network Information

The system provides functions of deletion and storage of network information.

8.7 Management of Random Interception

8.7.1 Task Management of Random Interception

The system can establish a random interception task, and configures monitoring module, monitoring range, and monitoring tasks (SMS and/or voice).

The user can also stop the current random interception task or restart the stopped task.

8.7.2 Real-Time/Quasi-Real-Time Decryption of the Random Interception

For encrypted conversation the network intercepted by the random interception, the system automatically decrypt according to its encryption modes in real time or quasi real time, recovering the signaling information, voice and SMS, etc in the communication.

8.7.3 Voice Monitoring by the Random Interception

The system is able to monitor frequencies on the frequency list of the current appointed location, and intercept one or multiple lines of conversations at the frequencies monitored, and can play certain line of conversation requested by the user.

8.7.4 Automatic Storage and Management of Voice Monitored by the Random Interception

The system can automatically store voice information (some of the information may

not be provided by the network) that is intercepted, including:

- *In/Out*
- *Focus，target or not*
- *IMSI/TMSI*
- *ISDN of the other party*
- *Start time*
- *Receiving time*
- *Duration of the call*
- *Operator*
- *LAC*
- *CI*

In addition, the system can extract, delete, change format of, and replay the stored voice files.

8.7.5 SMS Interception by the Random Interception Function

The system can monitors all the frequencies on the list of the current location of the system, intercepting sending and receiving of SMS on the frequencies monitored, and displaying the SMS on the screen. The monitored SMS information (some of them may not be provided by the network) includes:

- *Interception time*
- *R/S（receiving SMS or sending SMS）*
- *IMSI/TMSI*
- *ISDN of the other party*
- *SMS contents*
- *Cell information*
- *Device intercepted*

8.7.6 Automatic Storage and Browsing of SMS Monitored by the Random Interception Function

The system automatically saves the SMS information intercepted in to a Microsoft Office Excel for further checking; and provides function of deleting SMS display on

the screen by real time.

8.8 Management of Specific Target Interception

8.8.1 Management of Specific Target Interception

The system can establish an interception of a specific target, and configures monitoring module, monitoring range for it.

In addition, the system can stop the current interception task and restart the stopped one.

8.8.2 Real-Time/Quasi-Real-Time Decryption of Specific Target Task

For encrypted conversation intercepted during monitoring of specific target, the system will automatically decrypt it according to the encryption modes by real time or quasi real time, recovering traffic such as signaling information, voice and SMS in communication.

8.8.3 Manual Capturing of Specific Target

Users can manually triggers the appointed target by concealed SMS and capture it to obtain the current network information (some of the information may not be provided by the network):

- *TMSI/IMSI*
- *Kc*
- *Current Cell*
- *Rough distance to the target*

8.8.4 Automatic Capturing of Specific Target

The system provide auto scanning method to capture the appointed target, scanning parameters include:

- *Its operator*
- *The smallest RSSI value*
- *Target's ISDN*
- *Type of Concealed SMS Triggering*
- *Monitoring Modules Number per each cell*

- *The triggering SIM card number*
- *Retrying number if the triggering fails*
- *Interval between SMS triggering*
- *Number of SMS triggering*
- *Delay of concealed SMS in the network*

8.8.5 Monitoring of Specific Target's Voice

The system can monitors frequencies in the frequency list for the current location of the system, can intercept target's newly started voice call and replay it.

8.8.6 Automatic Storage and Management of Specific Target's Voice

The system can automatically stores intercepted voice information (some of the information may not be provided by the network of specific targets including:

- *In/Out*
- *Focus，target or not*
- *IMSI/TMSI*
- *ISDN of the other side*
- *Start time*
- *Receiving time*
- *Duration*
- *Operator*
- *LAC*
- *CI*

In addition, the user can extract, delete, change format of and replay voice files.

8.8.7 Interception of Specific Target' SMS

The system can monitor appointed frequencies on the frequency list of the current location, and intercept specific target's SMS sending and receiving on the frequencies monitored and display those SMS on the screen. The monitored SMS information (some of the following information may not be provided by the network) includes:

- *Interception time*

- *R/S（receiving or sending）*
- *IMSI/TMSI*
- *ISDN of the other party*
- *SMS contents*
- *Cell information*
- *Device monitored*

8.8.8 Automatic Storage and Browsing of Specific Target's SMS

The system automatically saves the specific target's SMS information that is intercepted into Microsoft Office Excel for further checking; and the user can delete real time SMS on the screen.

8.8.9 Direction Finding (DF) of Specific Target

Under the specific target interception task, by triggering the specific target or SMS or who is in the progress of a call, the system will automatically and covertly measures uplink signals to get the direction of the target, and at the same time provides current Intensity value of the uplink signals of the target, which determines the rough distance to the target.

8.8.10 Processing and Recording of Specific Target's DF Results

Under the specific target task mode, the system can find direction of the target and get the following results:

- *Azimuth angle of the target's current location*
- *Intensity of the target's uplink signals*
- *Reliability of current direction finding results*

8.8.11 Sending of Specific Target's DF Results to the Front-End Screen

Under the specific target task mode, the system sends results information of each direction finding to the front-end screen on the vehicle subsystem, so that the driver of the vehicle subsystem can decide driving route accordingly.

8.8.12 Display of Current Location on GIS Map

After calibration of GIS, the current location of the vehicle subsystem will be displayed on the GIS map which is helpful for the driver. In addition, users can open,

close, drag, zoom in and out, and let the map move automatically while the vehicle is static.

8.8.13 Adding of DF Results on the GIS Map and Assisted Positioning

Under the specific target task mode, results of each time of direction finding can be managed and added to the GIS map. DF results including:

- *NO.*
- *Time*
- *Place*
- *Intensity*
- *Vehicle's Angle*
- *DF angle*
- *Range*
- *Longitude*
- *Latitude*

According to results obtained on different locations, the system can find the rough location of the target by its unique computing method and notes the location on GIS map for determination by the system operators.

In addition, the system provides layer management function, including adding, deletion, display and hide of it.

9 Detailed Description of Functions of the Fixed Station Subsystem

9.1 Management of Monitoring Devices

9.1.1 Checking of Versions of Monitoring Unit's Hardware and Software

The system provides checking of serial numbers of monitoring modules in the monitoring unit, and version information of its hardware and software, including:

- *Serial numbers of monitoring modules*
- *Version Information of hardware*

- *Version information of software*

9.1.2 Turning on and off of Monitoring Unit

Users can turn on and off all the monitoring modules in the monitoring unit.

9.1.3 Checking Status of the Monitoring Unit

Users can browse the following information about monitoring modules of the monitoring unit in real time:

- *Turning off (by this time, all the information about modules is unknown)*
- *Idle (all the modules are ready to work, namely the status is ok)*
- *Status of Frequency scanning (when the status of modules are FCCH Scanning)*
- *Status of Signaling Tracking; by this time, the status of modules including:*
  - *WSYN: indicates that the module is synchronizing with the appointed frequency point;*
  - *AGCH: indicates that the module is monitoring network on certain frequency point;*
  - *SDCCH: indicates that the module follows some conversation on some frequency point and is entering into SDCCH channel*
  - *TCH: means that the module has already entered into some speech channel.*

9.1.4 Task Operations on Monitoring Unit

According to task requirements, the system provides monitoring modules with the following operations:

- *Start task*
- *Release task*
- *Restart task*

9.2 Management of Triggering Device

9.2.1 Checking Status of the Triggering Device

Users can browse the following status of the target triggering device which triggers the target covertly.

- *IMEI (identity) of the triggering device*
- *Name of the triggering device*
- *IMSI of the SIM card*
- *Current network signal intensity on the triggering card*
- *Current status of the triggering card*
  - *Idle*
  - *Ringing or dialing*
- *The last missed call*
- *If new SMS is received*

9.2.2 Simulation of Mobile Phone by the Triggering Device

The triggering device can simulate mobile phone can conduct the following functions (different models of triggering devices may differ in functions):

- *Browsing received SMS*
- *Delete some or all received SMS*
- *Establish and send SMS*
- *Receive new SMS, and prompt the receiving*
- *Prompt of incoming call*
- *Receive or refuse a call*
- *Tuning of voice volume*

9.3 Cell Information Scanning

9.3.1 Scanning Information on Full Frequency

The system provides scanning of all the frequency points on the GSM 900/1800MHz, the scanning results include;

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value，the unit is second*

9.3.2 Scanning Information of an Appointed Operator

On both of the GSM900/1800MHz ranges, the system can scan frequencies of an appointed telecom operator, and obtain all the frequency information of the current location, including:

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value, the unit is second*

9.3.3 Scanning Information of the Appointed Frequencies

On both of the GSM900/1800MHz ranges, the system can scan an appointed frequency point or range. The scanning results include:

- *FCCH value*
- *CA list*
- *RSSI value*
- *Operator*
- *CI*
- *LAC*
- *TTL value, the unit is second*

9.3.4 BER Testing

According to the frequency scanning results or an appointed frequency range, the system conduct BER testing to all the frequency points based on statistic time length, BER report cycle, and show the testing results on the frequency list.

9.4 Local Information Management

9.4.1 Output of Information from Monitoring Modules

By local information management, the system output operation and status information of all the monitoring modules, including: turning on and off of modules, frequency scanning, start of a task, task implementation, etc.

9.4.2 Deletion and Storage of Local Information

The system provides functions of deletion and storage of local information.

9.5 Management of Network Information

9.5.1 Output of Monitoring Modules' Network Information

To the network information the system outputs various kinds of information about monitoring modules including:

- *Frequency monitoring information, namely frequency points the monitoring modules are monitoring;*
- *The network information are found: including TMSI, IMSI, calling ISDN number;*
- *Network synchronization information: synchronization and lost of synchronization with all the frequency points in the network;*
- *Network signaling information, including handover and hang-up.*
- *The information generates when the module enters into TCH and when follows target into cell handover.*

9.5.2 Deletion and Storage of Network Information

The system provides functions of deletion and storage of network inform

9.6 Management of Random Interception

The fixed station subsystem has specially optimized the scheduling algorithms for multiple modules and alternation of decryption processing to dramatically increase concurrency of random interception, comparing with the random function of the vehicle subsystem.

9.6.1 Task Management of Random Interception

The system can establish a random interception task, and configures monitoring module, monitoring range, and monitoring tasks (SMS and /or voice).

Users can also stop the current random interception task or restart the stopped task.

9.6.2 Real-Time/Quasi-Real-Time Decryption of the Random Interception

For encrypted conversation the network intercepted by the random interception, the system automatically decrypt according to its encryption modes in real time or quasi real time, recovering the signaling information, voice and SMS, etc in the communication.

9.6.3 Voice Monitoring by the Random Interception

The system is able to monitor frequencies on the frequency list of the current appointed location, and intercept one or multiple lines of conversations at the frequencies monitored, and can play certain line of conversation requested by the user.

9.6.4 Automatic Storage and Management of Voice Monitored by the Random Interception

The system can automatically save voice information (some of the information may not be provided by the network) that is intercepted, including:

- *In/Out*
- *Focus，target or not*
- *IMSI/TMSI*
- *ISDN of the other party*
- *Start time*

- *Receiving time*
- *Duration of the call*
- *Operator*
- *LAC*
- *CI*

In addition, the system can extract, delete, change format of, and replay the stored voice files.

9.6.5 SMS Interception by the Random Interception Function

The system can monitors all the frequencies on the list of the current location of the system, intercepting sending and receiving of SMS on the frequencies monitored, and displaying the SMS on the screen. The monitored SMS information (some of them may not be provided by the network) includes:

- *Interception time*
- *R/S（receiving SMS or sending SMS）*
- *IMSI/TMSI*
- *ISDN of the other party*
- *SMS contents*
- *Cell information*
- *Device intercepted*

9.6.6 Automatic Storage and Browsing of SMS Monitored by the Random Interception Function

The system automatically saves the SMS information intercepted in to a Microsoft Office Excel for further checking; and provides function of deleting SMS display on the screen by real time.

9.7 Management of Specific Target Interception

9.7.1 Management of Specific Target Interception

The system can establish an interception of a specific target, and configures monitoring module, monitoring range for it.

In addition, the user can stop the current interception task and restart the stopped one.

9.7.2 Real-Time/Quasi-Real-Time Decryption of Specific Target Task

For encrypted conversation intercepted during monitoring of specific target, the system will automatically decrypt it according to the encryption modes by real time or quasi real time, recovering traffic such as signaling information, voice and SMS in communication.

9.7.3 Manual Capturing of Specific Target

Users can manually triggers the appointed target by concealed SMS and capture it to obtain the current network information (some of the information may not be provided by the network):

- *TMSI/IMSI*
- *Kc*
- *Current Cell*
- *Rough distance to the target*

9.7.4 Automatic Capturing of Specific Target

The system provide auto scanning method to capture the appointed target, scanning parameters include:

- *Its operator*
- *The smallest RSSI value*
- *Target's ISDN*
- *Type of Concealed SMS Triggering*
- *Monitoring Modules Number per each cell*
- *The triggering SIM card number*
- *Retrying number if the triggering fails*
- *Interval between SMS triggering*
- *Number of SMS triggering*
- *Delay of concealed SMS in the network*

9.7.5 Monitoring of Specific Target's Voice

The system can monitors frequencies in the frequency list for the current location of the system, can intercept target's newly started voice call and replay it.

9.7.6 Automatic Storage and Management of Specific Target's Voice

The system can automatically stores intercepted voice information (some of the information may not be provided by the network of specific targets including:

- *In/Out*
- *Focus，target or not*
- *IMSI/TMSI*
- *ISDN of the other side*
- *Start time*
- *Receiving time*
- *Duration*
- *Operator*
- *LAC*
- *CI*

In addition, the user can extract, delete, change format of and replay voice files.

9.7.7 Interception of Specific Target' SMS

The system can monitor appointed frequencies on the frequency list of the current location, and intercept specific target's SMS sending and receiving on the frequencies monitored and display those SMS on the screen. The monitored SMS information (some of the following information may not be provided by the network) includes:

- *Interception time*
- *R/S（receiving or sending）*
- *IMSI/TMSI*
- *ISDN of the other party*
- *SMS contents*
- *Cell information*

- *Device monitored*

9.7.8 Automatic Storage and Browsing of Specific Target's SMS

The system automatically saves the specific target's SMS information that is intercepted into Microsoft Office Excel for further checking; and the user can delete real time SMS on the screen.

10 Detailed Description of Individual-Soldier Subsystem's Functions

10.1 Turning on and off of Transmission Device of Individual-Soldier Subsystem (On the Vehicle Side)

The user can turn on and off the individual-soldier subsystem on the vehicle side. The system provides shortwave power amplifier to remotely command the individual-soldier subsystem to approach the target under specific target task.

10.2 Turning on and off of Individual-Soldier Subsystem (Individual-Soldier Side)

There is power on and off switches on the individual-soldier side; and self-examination function to check if the system works normally.

10.3 Connection of Bluetooth Transceiver on the Individual Soldier Side

The Bluetooth transceiver is employed on the individual-soldier side (better concealment of Bluetooth transceiver when the operator is closely approaching a target). The individual-soldier side device supports connection to a Bluetooth transceiver to make sure that the operator can obtain measure information of the target to get closer to him.

10.4 Communication between Individual Soldier Subsystem and the Vehicle Subsystem

The individual-soldier subsystem should communication with the vehicle subsystem in order to approach the target. Information interacted between the two includes: frequency point of the target, start time of the conversation, channel parameters of the target's uplink signal.

10.5 Determination of Target's Direction by Values in Triggering SMS

When the individual-soldier subsystem is approaching a target, based on relative information sent by the vehicle subsystem, it measures intensity of the target's uplink signals with its directional panel antenna and obtain intensity value to judge the rough distance of the target; According to measuring of target uplink signal intensity from all the directions of a specific target, the operator can judge direction of the target and get closer to him.