Flare®

Personal Alarm Locating System

Technical Manual

Gen 2 IP-Based Sensors

T1DA1802-001 Rev C
May 16, 2018

SENSTAR™

Senstar Corporation
Website: www.senstar.com
Email address: info@senstar.com

T1DA1802-001, Rev. C
First edition
May 16, 2018

Senstar Corporation has prepared the information provided in this guide to the best of its ability. Senstar Corporation is not responsible for any damage or accidents that may occur due to errors or omissions in this guide. Senstar Corporation is not liable for any damages or incidental consequences arising from the use of, or the inability to use, the software and equipment described in this guide. Senstar Corporation is not responsible for any damage or accidents that may occur due to information about items of equipment or components manufactured by other companies. Features and specifications are subject to change without notice. Any changes or modifications to the software or equipment that are not expressly approved by Senstar Corporation void the manufacturer’s warranty, and could void the user’s authority to operate the equipment.

This document is for software versions 1.750 and higher.

Senstar Corporation’s Quality Management System is ISO 9001:2015 registered.

Senstar intellectual property is protected by the following patents:

Canada: 2,225,638

U.S. 5,977,913

Compliance:

Canada:

FCB Technical Acceptance Certificate No. 1454B-T1FG1601

United States:

FCC Grant of Equipment Authorization FCC Identifier 15TT1FG1601

List of acronyms

CMPC	Central Monitoring Post Computer – the Flare PC
DNR	Did not respond – (result of a MiST)
FPD	Fixed Protection Device – (stationary Personal Protection Device)
MaST	Major Self-test
MiST	Minor Self-test
NM	Network Manager
NMPC	Network Manager Personal Computer – NM often runs on the Flare PC
OOR	Out of Range
PALS	Personal Alarm Location System – (Flare system) Portable Alarm Location System – (alternate term for Flare system)
PoE	Power over Ethernet: network communication switch and power supply for Su’s and SaTU’s
PPA	Personal Portable Alarm – (alternate term for PPD)
PPD	Personal Protection Device – personal alarm transmitter (PPA)
RSSI	Received Signal Strength Indication
SaTU	Sensor and Test Unit
SMS	Security Management System
SSA	Single Sensor Alarm
SSNR	Signal Strength No Response
SU	Sensor Unit – the receiver (Sensor)
UCM	Universal Configuration Module (software application)
VM	Virtual Machine

List of definitions

Backbone: The communication network (typically fiber optic) between the CMPC and the PoE switches.

Decode Drop Out: The RSSI level under which a sensor cannot consistently decode a PPD’s or FPD’s modulated signal.

Noise Floor: The RSSI alarm threshold, a running calculation approximated by
NF = noise level + RSSI Step Size.

Sensor Network: The Ethernet-based network between the PoE switches and sensor units.

Related Publications

T1DA1003-001 Gen 2 PPD Setup

T1DA1203-001 Installing Outdoor Antennas

T1DA1403-001 Installing Gen 2 IP-Based Sensors

T1DA1602-001 System Administrator Manual

Table of Contents

1 System Overview

This document includes descriptions and setup details for Flare system components, including device settings, addressing, network setup and diagnostics. For information on the Flare system software, refer to the Flare System Administrator manual (T1DA1602).

The Flare Personal Protection Device (PPD) is a small, portable belt-worn UHF transmitter that is assigned to facility personnel such as correctional officers and health care professionals. The Flare transmitter is also available as a wireless Fixed Protection Device for use as a panic or duress button. In alarm situations the PPD is activated and transmits a signal, which is received, decoded, and processed by a distributed network of RF receivers (sensors). The data from the sensors is then forwarded to the Flare Central Monitoring Post Computer (CMPC) where the data is analyzed and the location of the transmitter is determined. The location of the alarm is displayed on a facility map presented on the CMPC. The Flare alarm data can also be communicated to a third party security management system (SMS).

1.1 PPD Alarms

By default, the PPD will transmit the following alarm types:

Push-Button

> The PPD transmits an alarm message when the red push-button is pressed.

Low Battery

> The PPD automatically transmits a low battery message when the battery drops below a certain voltage. Each subsequent activation of the PPD will retransmit the low battery message until the battery is replaced.

Optionally, PPD Transmitters can also be configured to use one or both of the following methods of activation:

Man-Down (Tilt)

> The PPD transmits an alarm message when the unit is tilted beyond a specified setting for a preset period of time. The tilt sensitivity, and delay times are administrator programmable.

Pull-Pin (Tamper)

> The PPD transmits an alarm message every few seconds when a pull-pin is removed from the unit. The pull-pin lanyard is typically looped around the wearer’s belt. The pin is pulled out of the PPD if the PPD is forcibly removed from the wearer.

Self-Test (test transmission)

> The PPD transmits a test alarm message to verify operation (see the PPD User instruction T1DA1003). Due to the activation method, Self-Test cannot be used on PPDs that use the Man-Down alarm.

1.2 FPD Alarms

The FPD will transmit the following alarm types:

Push-Button

The FPD transmits an alarm message when the push-button is pressed.

Low Battery

The FPD automatically transmits a low battery message when the battery drops below a certain voltage. Each subsequent activation of the FPD will retransmit the low battery message until the battery is replaced.

1.3 Flare System Components

The Flare system is typically comprised of the following components:

PPD	Personal Protection Device: RF transmitter, aka. Personal Portable Alarm (PPA)
FPD	Fixed Protection Device: RF transmitter available as a wireless fixed point alarm (panic or duress buttons)
SU	Sensor Unit: an RF receiver (aka Sensor)
SaTU	Sensor and Test Unit: a sensor that is also configured to send a PPD type transmission to test nearby system receivers
CMPC	Central Monitoring Post Computer: the PC running the Flare software application (typically also runs the Network Manager and UCM applications)
PoE	Power over Ethernet: network communication switch and power supply for SUs and SaTUs

1.3.1 Personal Protection Device (PPD)

The PPD is an RF transmitter that transmits an administrator programmable modulated code ID when activated. The PPD can also be configured to include man-down activation, pull-pin activation, dual frequency transmission, and multi-broadcast transmission. A self-test option is also available, but cannot be used in conjunction with the man-down alarm. The PPD transmits a low battery alarm when its battery voltage drops below a certain voltage. PPD IDs range from 0 - 65535. The default PPD ID is the last 3 digits of the unit’s serial number.

Note In order to use the dual frequency and/or multi-broadcast options at a site, the setting(s) must be enabled on all Flare devices (PPDs, SUs and SaTUs).

1.3.2 Fixed Protection Device (FPD)

The FPD is a a fixed position version of the PPD. The man-down, pull-pin and self-test features are not used on the FPD. All other functionality, including programming, is done in the same way using the same tools as with the PPD. The remainder of this document will refer only to the PPD unless items specific to the FPD are being discussed.

1.3.3 Sensor Unit (SU)

The sensor unit consists of RF transceivers, microprocessor, and communications interfaces (USB and Ethernet). Flare installations typically include 100 to 300 sensors, which are strategically distributed throughout the facility. When an SU detects a PPD alarm transmission, it measures the strength of the received signal and provides a normalized Received Signal Strength Indication (RSSI). A single PPD transmission is received by many sensor units. The SUs provide RSSI information to the Flare software via the Network Manager for location analysis. Each sensor is connected to a class 3 PoE switch via Cat 5e cable, and must be located within 100 m (328 ft.) of the switch to which it is connected. Flare systems include multiple PoE switches (one or more per building, as required) which are in turn connected to a central switch located in the control equipment room. The inter-building connections are typically via fiber optic cable. See Installing SUs on page 29.

1.3.4 Sensor and Test Unit (SaTU)

The Sensor and Test Unit (SaTU) is a sensor unit that is configured in the Flare database to send a PPD type test transmission to verify that nearby SUs are functioning properly. SaTUs are defined throughout a site to test and verify individual groupings of SUs. During system tests, the Flare software activates the SaTU's test transmission. The Flare software verifies that nearby sensors received the SaTU transmission and compares the results to previously recorded RSSI levels.

Note There is no physical difference between a SaTU and an SU. A SaTU is an SU that has been configured via the UCM to activate test transmissions. An SU that uses external/outdoor antennas cannot be used as a SaTU.

1.3.5 Central Monitoring Post Computer (CMPC)

The Flare software application runs on the CMPC, which is a PC running a Windows-based operating system. The CMPC communicates with the distributed SUs via the Network Manager. It controls the operations of the system components and applies the locating algorithm on the signal strength measurements received from the SUs during an alarm event. The Flare software determines the location of the PPD alarm transmissions and presents the alarm location to the user on graphical layouts of the facility. An audible alarm is also generated. Optionally, the CMPC can output alarm location messages to an external security management system via Starcom or DWI protocol. The Flare software provides functions to configure the system, calibrate the system, set or modify various system parameters, and conduct various system diagnostic tests.

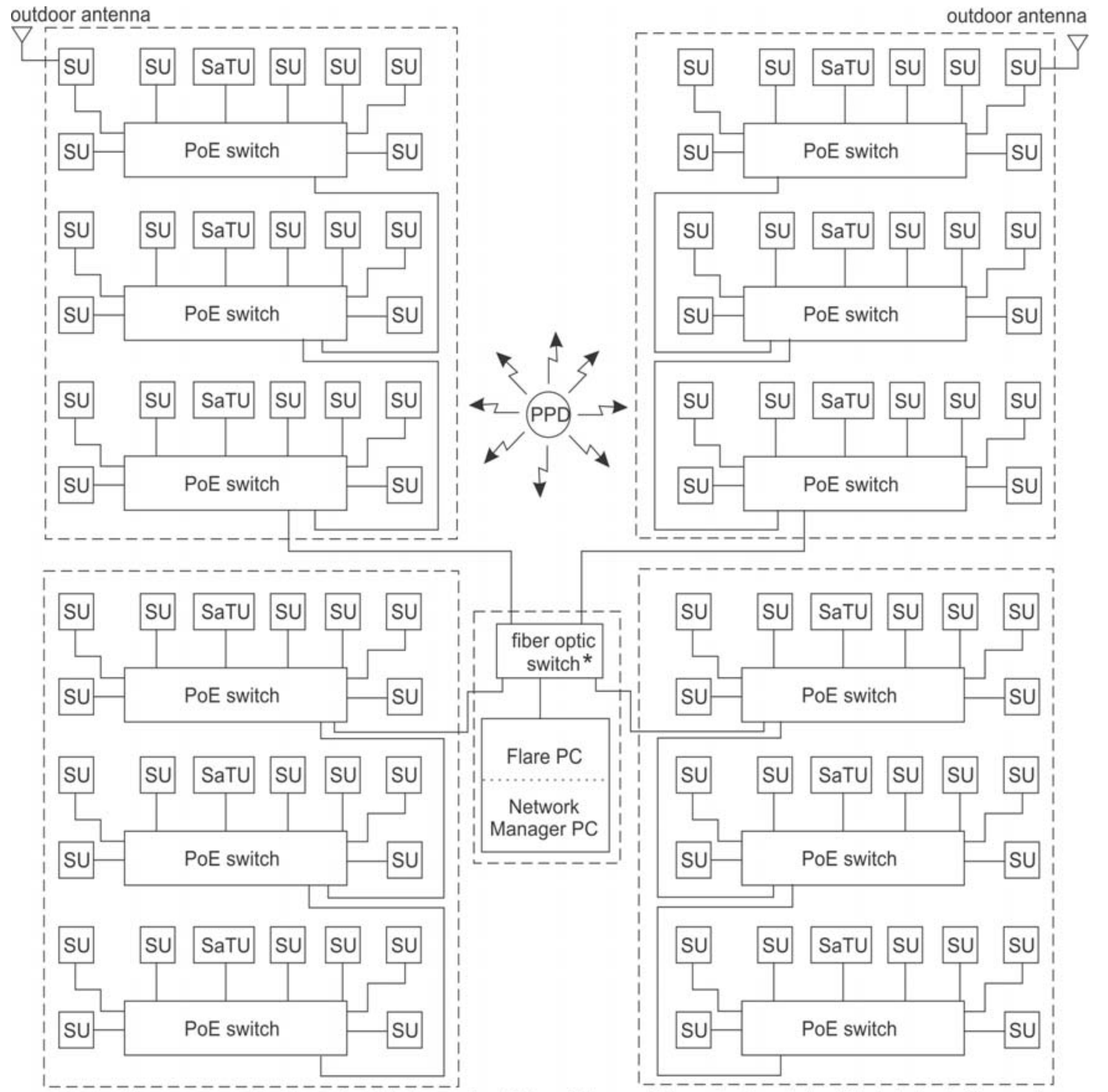
Note Contact Senstar Customer Service for information about forwarding Flare alarm data to 3rd party security management systems.

The NM and UCM are usually run on the CMPC. The NM and UCM can also be run on a separate PC that can be connected to the network to perform NM front panel or UCM diagnostics remotely, without disturbing the CMPC operator.

1.3.6 PoE Switch

The Flare sensors are powered by, and communicate through a class 3 PoE switch. Each connected sensor must be located within 100 m of its PoE switch, and Category-5e wiring is required. When multiple PoE switches are used at a site, they are usually connected to a central switch located in the control equipment room. The CMPC is also connected to the central switch.

The following figure is a block diagram of a Flare system covering four three level buildings and a large outdoor area.



*The backbone communication network between the PoE switches and the central control switch is typically fiber optic. The communication network between SU's and SaTU's to the PoE switch is category 6 cable.

Figure 1: Conceptual Flare system block diagram

2 Flare System Setup

Sensor unit configuration is done via the Universal Configuration Module (UCM) software. Prior to installing an SU, you must setup its unique IP address and subnet mask. For SU installation, configuration and setup details refer to T1DA1403 Installing Gen 2 IP-Based Sensors. If you are using external or outdoor antennas, refer to T1DA1403 Installing Outdoor Antennas.

Note For most Flare installations, SU setup requires only that each SU be assigned a unique IP address and a common subnet mask. In addition, before installation each SU should be tested to ensure proper reception of PPD transmissions (see T1DA1003 Gen 2 PPD Setup). The SUs can then be installed and their locations and IP addresses can be noted on a site plan.

Note The PC used to setup the IP addresses for the network devices must be on the same subnet as those devices (you may need to change the PCs IP settings, see T1DA1403 Installing Gen 2 IP-Based Sensors).

2.1 System Implementation

The following procedure provides a guide to implementing a Flare system:

1. Create a table similar to the example table below for use as a system configuration document and assign each device a unique IP address (by location).
2. Set the IP address and subnet mask of each device and label the device to ensure it goes to the correct installation location.

Note This includes setting the IP addresses of the switches, PCs and SUs.

3. Install each device. Using a laptop with the UCM and NM, confirm communications to each sensor on a network by connecting the laptop to each switch. Confirm communications as you go by adding each additional sensor node definition (sensor type and IP address) to the NM front panel. Define each sensor node under the NM Configure Nodes tab. Save and restart with each change.
4. Install the UCM, NM and Flare software on the CMPC and connect the CMPC to the network.
5. Setup the Flare database to communicate with the sensor hardware (see T1DA1602 System Administrator manual).
6. Calibrate the SaTUs and run commissioning type interval SaTU testing (see T1DA1602 System Administrator manual).
7. Calibrate the System and test for location accuracy.

The following table provides an example of the IP address ranges used for a Flare system:

Type of Equipment	Equipment	IP Address Range	Subnet Mask
Computer	Flare PC	172.16.96.1 through 172.16.96.19	255.255.252.0
Networking Equipment	Fiber Switches	172.16.96.20 through 172.16.96.39	255.255.252.0
Networking Equipment	POE Switches	172.16.96.40 through 172.16.96.200	255.255.252.0
Networking Equipment	Other site-specific networking related equipment	172.16.96.200 through 172.16.96.254	255.255.252.0
Flare Sensors	Flare Sensors	172.16.97.1 through 172.16.97.200 172.16.98.1 through 172.16.98.200 172.16.99.1 through 172.16.99.200 172.16.100.1 through 172.16.100.200	255.255.252.0

2.2 Network Switch Setup

The network switches and other network devices must be configured and setup for use with the Flare system.

Note The following procedure provides an example setup for a PoE Switch. Refer to the manufacturer's documentation for the specific procedure for the switches and other network devices used on-site.

1. Using an Ethernet cable, connect a PC to the PoE Switch using one of the ports on the front of the switch.
2. Determine the IP address of the switch (factory default - e.g., 192.168.0.239).
3. Setup the computers IP settings to be on the same Subnet as the switch:
   e.g., IP Address: 192.168.0.1
   Subnet Mask: 255.255.255.0
4. Using internet explorer, type the IP address of the switch in the address bar.
5. Login to the switch using the default password.
6. Under the "System" Tab, ensure "Management" is selected. Select "IP Configuration".
7. Change the IP address of the switch to a Static IP Address.
8. You will then be able to set the IP address on the screen.
   Suggested settings are as follows (It is very important to write these settings down):
   IP Address: 172.16.96.40 (use a different IP address if this one is in use at this site).
   Subnet Mask: 255.255.252.0
9. Accept the changes to the switch.
10. Setup the computer's IP settings to the following:
    IP Address: 172.16.96.1.
    Subnet Mask: 255.255.252.0
11. Using internet explorer, type the IP address of the switch in the address bar.
    (In the previous steps, we set this to 172.16.96.40.)
12. Login to the switch using the default password.

13. Under the “System” Tab, ensure “Management” is selected. Select “Network Interface”.
14. Verify that the IP address that was set is as expected.
15. Under the “Switching” Tab, ensure “Ports” is selected. Select “Port Configuration.”
16. Using the checkboxes, select all ports to which an SU is connected.
17. Using the drop-down box, change these to have a port speed of “100 Mbps Half Duplex”.
18. Select “Apply”.
19. Select “Logout”.

2.3 Universal Configuration Module (UCM)

Setup and configuration of the PPDs and SUs are done with the Universal Configuration Module (UCM) a Windows-based software application (00SW0100). The UCM also provides diagnostic, monitoring and maintenance functions for each Network based device. The UCM can reside on the same PC as the NM, or can be located on a separate computer. The UCM connects to the NM using TCP/IP, and through the NM, can communicate with any SU on the Network without interrupting other network functions. The UCM can also connect directly to each sensor via USB.

The Network Manager must be configured to accept a UCM connection (under the NM’s Configure UCM tab). Each NM allows up to 5 UCM connections (4 remote and 1 via the local host; 127.0.0.1).

2.4 Network Manager

The Network Manager (NM) handles the alarm data management for Senstar’s proprietary security networks (Krypton, Silver, FiberPatrol, CCC, and Crossfire networks). The Network Manager is available as a Windows Service on the Network Manager Suite CD (00FG0220). The NM functions as a data server which collects and distributes alarm data and control functions for the Flare system software.

Note	To maintain the prompt system response required by the Flare life safety application, DO NOT install and run the Network Manager on a virtual machine (VM). Fast response on a VM can be problematic due to its handling of timed events.

The Network Manager controls and manages the Network of Flare devices. A Flare system can have up to four NMs, with each controlling a Network of up to 200 Flare sensors. The NM communicates with Senstar’s Flare System software via a TCP/IP link using the Network Manager Interface (NMI). The Network Manager usually resides on the same PC as the Flare software to which it reports, but can also reside on another PC.

- To link the NM to Flare, specify the IP address of the Flare PC in the NM Configure SMS tab > TCP/IP tab.

For redundant applications, two identical Network Managers are setup on two separate computers.

- To enable redundancy, under the NM Configure Redundancy tab, define the mate NM PC’s IP address, and set one NM as Primary.

The two computers must be connected via Ethernet to determine which NM is active. The primary NM communicates with the network devices and the Flare software. If the primary NM goes off-line, the redundant NM becomes active and takes over. When the primary NM comes back on-line, it runs in standby mode.

2.5 Flare Software

Install the Flare software by inserting the CD into the drive and using Windows Explorer to run the copyFiles.bat command on the CD. If there is a Flare database available, load the database by copying the files into database folders as set in the Flare.ini file. This section provides an overview of the files that comprise the Flare software system. The Flare software system has two main elements:

Application Software	(FlareVxxxx.exe, xxxx = the version) and configuration settings file (Flare.ini)
System Database:	floor map files (*.emf or *.bmp) and calibration data files: database type 0: *.arc files database type 1: *.mdb file

Use the MPIUs dialog to define the Network Manager(s). Set the port number (ranging from 850 to 853 for NMs 1 to 4), select Kr NM from the drop down menu and enter the IP address for the Network Manager PC.

Use the Hot Standby property page in the Flare software to configure redundant Flare PCs.

“MPIUs Are Active” determines if the Flare application is on line with the Flare networks. Inactive mode is used for demonstration purposes and during database creation. If inactive, Flare will ignore received messages and inhibit transmitting messages to the Flare networks.

2.5.1 Flare Files Directory Structure

Flare system software and support files are contained in a local disk (C:) folder named Flare, or FlareVxxxx (with the version number appended, e.g., FlareV1750). The following example uses the name Flare, resulting in a folder C:\Flare. Map files can be either emf or bmp file types. In this example, emf files are used.

```
C:\Flare\
FlareVxxxx.exe
Flare.ini
prison1\
    map files (prison1.emf and floor system emf files)
    current\
            type 0 database and calibration arc files (including prison1.arc)
            type 1 database and calibration mdb file
    logs\
            OPS logs
            DIAGS logs
            ALRMS logs
            SaTU_test_data\
                    Contains SaTU test data log files.
```

The ini setting MapPath determines the map folder and sitename, this sets the main map (site plan) filename and main database file. For the default site name, prison1, the map folder is C:\Flare\prison1, the main map file is C:\Flare\prison1\prison1.emf and the main database file is C:\Flare\prison1\current\prison1.arc.

However, the Flare file structure can also be customized using the new ini file settings for sitename, MapPath (e.g., C:\Flare\sitename\maps) and ArcPath (e.g., C:\Flare\sitename\arcs) for a more definitive structure:

```
C:\Flare\
    FlareVxxxx.exe
    Flare.ini
    sitename\
            maps\
                            map files (sitename.emf and floor system emf files)
            arcs\
                            type 0 database and calibration arc files (including sitename.arc)
                            type 1 database and calibration mdb file
    logs\
            OPS logs
            DIAGS logs
            ALRMS logs
            SaTU_test_data\
                    Contains SaTU test data log files
    Ophex\ (Device firmware files)
    SystemInfo\ (Device data files)
```

2.5.2 System Database

The database consists of two types of files: map files and data files.

Map Files

The map files are enhanced metafile format (.emf) or bitmap format (.bmp). There is one file for the main site map and as many other files as required for all floors of each building and the outdoor zones that make up the Flare locating coverage area. The sitename is user defined in the Flare.ini file and it determines the main map (site plan) filename. The indoor floor layout file names must be in the format Buildingname_Floorlevel.emf. The outdoor protection zone map file names must be in the format Zonename_.emf.

The building names, floor names, and zone names that the Flare application uses in database setup and definition will appear as in these user-defined file names. There must be a map file present in the map directory for each building floor level and each outdoor protection zone before that floor or outdoor zone can be added to the Flare database. See the Flare System Administrator manual (T1DA1602) for additional details.

Data Files

A database uses either of two file types to store hardware configuration and calibration data.

Type 0 – arc file types:

The **arc** files are stored in a single folder (default name – current). For the default site name, prison1, the main database arc file is prison1.arc. There is also one arc file for each PZone, which contains PZone information and calibration data.

Type 1 – mdb file:

The **mdb** file holds all PZone and calibration data. The default file naming convention is sitename_yymmdd.mdb.

3 SU/SaTU Operations

3.1 Sensor Unit RF Receiver Operation

Sensor Units are distributed throughout the site to receive and decode PPD transmissions, and to pass the data on to the Flare software. The Flare sensor has two orthogonal RF receivers which provide received signal data to the digital section of the SU. The SU constantly monitors the received signals from both antenna channels to detect PPD activity. The SU uses integrated transceivers, to provide two-way RF capability. This enables each SU to function as a SaTU, if required (software controlled).

3.1.1 Received Signal Strength Indication (RSSI)

The RSSI is the level of RF energy being received by the SU. This is a measure of signal level converted into a digital value in the range of 0 to 255. Since there will be differences in electronics from one receiver to the next, the raw RSSI value is applied into a normalization offset so that every SU gives the same normalized RSSI value for the same received RF energy. This makes it possible to install and replace any sensor in any sensor location without affecting the recorded sensor response profiles (calibration data).

Practical RSSI values will be in the range 20 to 200. Below 20 is noise level and 200 represents a PPD activation extremely close to the sensor. The signal may be an expected in band PPD transmission, or a high power near or in band interference signal. Activations of a PPD inches from an SU will give an RSSI close to or at the saturation level of 255. This test is often performed to verify sensor operation and location.

3.1.2 Noise Floor (NF)

During normal operation, the sensor is constantly sampling RSSI to detect alarm signals. It uses polarization diversity (alternates sampling between its two orthogonal antennas) to reduce multipath effects. The RSSI level present when there is no active PPD transmission is the RSSI noise level. This is a result of very wide-band ambient RF noise that is always present in the environment.

3.1.3 Frequency of Operation

The RF receiver is frequency versatile. It has a digitally tuned synthesizer and can be set to a wide range of frequencies within the public safety band (450 MHz – 470 MHz). Each Flare system will have an assigned frequency that does not change, but occasionally, a replacement sensor may not be set to the correct site specific frequency of operation. Be sure to check this when replacing sensors.

Prior to operating Flare at a site, a license is required. This licensing is administered by either the Federal Communications Commission (FCC) in the United States, or Industry Canada (IC) in Canada. Senstar Technical support can assist with this licensing process. Once a site is licensed, other radios/transmitting equipment are not permitted to interfere with the Flare system, which is critical for life safety applications. At sites where there are 2 available frequencies (requires 2 licenses) PPDs and SUs can be configured for dual frequency alarm transmissions.

Note	In order to use the Dual Frequency and/or Multi-Broadcast options at a site, the setting(s) must be enabled on all Flare devices (PPDs, SUs and SaTUs).

4 Flare System Operations

4.1 Alarm Process

4.1.1 SU Alarm

In normal operation mode (PPD processing enabled) the sensor will constantly be checking for PPD alarms. The PPD range setting for SUs is system wide, and is determined by the range of PPD IDs used at the site. When an SU detects an alarm, it communicates the alarm message to the Network Manager. A PPD transmission will be received by many sensors.

Note	An SU with PPD processing disabled does not process alarms. PPD processing disabled is used for diagnostics.

4.1.2 Flare CMPC Operator Display and Control

The Flare software receives these alarm messages from the NM and groups them. The Flare software applies the received RSSI data from the sensors in alarm to the calibration data (pre-recorded sensor responses) and uses the location algorithm to report the location of the PPD alarm transmission.

4.1.3 System Inspection

The Flare software performs a Minor Self-Test (MiST) at user-defined intervals. The MiST monitors the Flare devices to ensure that they are online and are operating without any diagnostic errors. If the number of devices offline exceeds user-defined levels, the Flare software issues a system unstable alert to the operator. The operator should immediately notify maintenance of the system unstable condition.

The Flare software will perform a Major Self-Test (MaST) daily at a user-defined time. The MaST includes a MiST, and SaTU test. These tests check device status, and the RF operation and consistency of sensors.

4.1.4 Sensor and Test Unit (SaTU) tests

The SaTU performs 2 functions for the Flare system. During normal operation, it functions as a sensor unit, continually monitoring for PPD alarms. As a test unit, it transmits a PPD type alarm to test the RF operation of nearby sensor units. The Flare software performs a global SaTU test (activating all SaTUs) daily at a prescribed time. Each SaTU is activated in turn and RSSI data is collected from sensors the same way it is during an alarm. The RSSI data is then compared to the SaTU calibration data (pre-recorded SaTU activations during known good sensor operation) if differences exceed user defined test tolerances (drift settings) then the difference is flagged.

The comparison will depend on the SaTU calibration data being valid and representative of when all sensors are known to be operating optimally. Also, the test relies on the SaTU operating properly, a persistent drop in all sensor responses is indicative of a SaTU transmit power change due to relocation of unit or antennas. The user defined drift settings are very important to the value of this test. Set too high and changes are not as readily flagged, too low and small effects will draw unnecessary attention.

After all SaTUs have been activated the global test results are displayed. Review this summary first since it indicates results for all sensors. Individual SaTU test transmissions will be picked up only by the sensors that are in range of that SaTU. Distant SUs (sensors receiving no signal) are not being tested by that particular SaTU.

RSSI response differences can result from sensor changes or from faults, which is the primary focus of the test. Note that the ‘fault’ may be as simple as a wrong PPD range or frequency set in the sensor. These changes tend to be isolated (occur on only one sensor). Differences can also be caused by changes in the RF environment due to alterations in buildings and internal construction, sensor position and antenna orientation or connection. The number of sensors affected is proportional to the magnitude of the environmental change. This secondary focus indicates that there have been changes since the calibration and some location testing is warranted in that area. Note that if the area needs to be recalibrated, the SaTU(s) covering that area should also be recalibrated. If the response change occurs on all sensors that respond to the SaTU, then the SaTU may have changed in output level, position or antenna orientation.

4.1.5 Interpreting SaTU Test Results

The test results are in three formats, results for an automated test, results for a manual test and the global results summary (you can decrease the descriptive output by deselecting the Verbose checkbox). A sample SaTU test event excerpt from the PALS-DIAGSYYMM.log for an automated test is shown:

```
2016-03-29 13:13:35  Start Test SaTU 54 (TxID 881) 'SaTU54'
2016-03-29 13:13:38  Calculating Test Results SaTU 54
2016-03-29 13:13:38  Logging Test Data (37 sensors) SaTU 54
2016-03-29 13:13:38    Sensor   3: RSSI 175  Cal Ave  18, drift 157 exceeded tolerance 40.
2016-03-29 13:13:38    Sensor  35: RSSI  84  Cal Ave  41, drift  43 exceeded tolerance 40.
2016-03-29 13:13:38    Sensor  52: RSSI   0  Cal Ave 185, drift 185 exceeded tolerance 50.
2016-03-29 13:13:38    Sensor  54: RSSI   0  Cal Ave 144, drift 144 exceeded tolerance 50.
2016-03-29 13:13:38    Sensor  56: RSSI   0  Cal Ave 175, drift 175 exceeded tolerance 50.
2016-03-29 13:13:38    SaTU 54 Test: Sensor responses 14, drift stats: maximum 185,
                       average 54
2016-03-29 13:13:38    SaTU 54 Test: Sensor drift tolerance exceeded on 5 sensor(s)
2016-03-29 13:13:38    SaTU 54, Total sensor drift 762 exceeded tolerance 400
2016-03-29 13:13:38  End Test SaTU 54
```

The sample shows individual sensor drift events, summary and total sensor drift event. The error for sensor 3 shows the current reported RSSI 175 is much greater than the calibration average of 18. This indicates poor or out of date calibration data. The second event is similar. The next 3 events show current responses of zero indicating these sensors are no longer receiving signal and may need corrective action. The sensors can be verified by a close proximity PPD activation, and by adding some test cal samples to a location close to the sensor and inspecting if the response for that sensor has changed compared to previous cal data.

Note Make sure that these test samples are deleted after the inspection is complete.

The total sensor drift event is intended to determine that many sensors have small drift values that may not exceed the individual drift threshold**.** A manual test will show all sensor results, not just those that exceeded drift tolerances. For example it will include 'within tolerance events' as follows:

```
2016-03-29 13:28:15     Sensor   6: RSSI   0  Cal Ave   0, drift   0 within tolerance 40.
2016-03-29 13:28:15     Sensor   9: RSSI   0  Cal Ave   0, drift   0 within tolerance 40.
2016-03-29 13:28:15     Sensor  10: RSSI 184  Cal Ave 184, drift   0 within tolerance 40.
2016-03-29 13:28:15     Sensor  11: RSSI 187  Cal Ave 172, drift  15 within tolerance 40.
```

For sensors 6 and 9 with no response and no calibration average the SaTU is too distant to invoke a response and is a non-test. Some other SaTU test is required to verify those sensors. The automatic test will log changes over long periods of time, manual tests and review of results is recommended so that regular inspection of the results is performed. To aid in showing that all sensors have been tested the global SaTU test results summary is generated, here is a sample:

```
2016-03-29 12:56:18  Global SaTU test results:
2016-03-29 12:56:18   Sensor 3: WARNING: No In Range Response.
2016-03-29 12:56:18   Sensor 6: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 20: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 21: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 22: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 50: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 51: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 52: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 53: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 54: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 56: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 57: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 58: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 231: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 232: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 9: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 30: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 31: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 34: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 36: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 37: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 103: WARNING: No In Range Response.
2016-03-29 12:56:19   Sensor 110: WARNING: No In Range Response.
2016-03-29 12:56:19  Global SaTU test results: 14 GOOD, 23 Warning(s), 0 No data.
2016-03-29 12:56:19  End Global SaTU Test
```

This summary will show which sensors have not been tested by any of the system SaTUs. The result ‘No In Range Response’ indicates that the sensor did not give a non-zero in range response. This can mean that it exceeded drift threshold or that it gave signal response of zero to all SaTUs. In the latter case, the sensor is either out of range of all SaTUs, or has a faulty RF receiver. Check sensor operation by activating a PPD close to the sensor and reviewing the response level against expected levels. If the device has no RF response it will have to be replaced with a properly functioning unit. If calibration has already been performed with the unit not responding, then the unit must be deleted and then re-added to the database to remove all previous erroneous 0 level responses. Areas where the sensor would pick-up PPD transmissions should be recalibrated. Note that if the lack of the sensor did not result in location inaccuracies it may still be better to replace it to contribute to sensor redundancy. The last line of the global test summary lists the system totals:

GOOD: sensors that have an in-range response

Warnings: sensors that do not have an in-range response

No data: sensors that are offline

The RSSI data from the SaTU tests is also logged into a file for each SaTU. This will reside in the SaTU test data folder in the Flare logs folder,
e.g., logs/SaTU_test_data/SaTU055_100423_a.log. These files can be processed and reviewed to track sensor response changes over time.

4.1.6 Periodic SaTU recal

At key points in time, it is a good idea to start new SaTU test logs. This is done by updating the cal of each SaTU. The recommended method is to add a sample (if the sample space is full you can delete one, if necessary). In this way the new activation sample is compared with the previous and any sensor RSSI changes can be reviewed. If there are sensor RSSI changes that are not expected, the process is to review the sensor operation and delete the new sample which may have suspect sensor RSSI data.
Key points are:

1. After all hardware is online and before cal is started.
2. After cal is complete.
3. After any SaTU changes.
4. After any major change to sensor configuration.
5. Before system acceptance testing.
6. Periodically by the maintenance technician (e.g., each half year).

Note	Points 3 and 4 usually require the deletion of all previous samples since the changes to SaTUs or sensors will cause OOR errors.

4.1.7 Reduced Locating Accuracy

There are many factors that could affect the system’s ability to accurately locate a PPD transmission. Problems related to the system’s ability to locate alarms are generally caused by one of these circumstances:

- Failure of one or more sensors in or near the area (offline, receiver loss of sensitivity, antenna changes, corrupt internal data).
  The system generally has enough redundancy so that a single sensor failure does not severely affect the ability to locate. However, there may be isolated areas where one sensor is heavily relied upon for accuracy and its failure limits the locating ability in those areas. This situation is compounded if two or more sensors in close proximity to each other are failing.

- Physical changes in the environment causing response differences from the calibration data.
- RF interference or noise causing false triggers or jamming the reception of some sensors.
- Inaccurate or poorly recorded calibration data for that area.
  This is especially true if the area in which the system fails to work is very small (a single room, closet, stairwell, etc.).
- Corrupt or unloadable calibration data.

The main problem is determining if it is the system or the environment. The first step in diagnosing such a problem is to verify the basic integrity of the system by completing both MiST and SaTU tests. These tests will help diagnose causes 1 to 3. Also, perform location accuracy tests with more than one PPD to rule out PPD ID range issues or other configuration errors.

If a sensor is defective or communications are impaired, the MiST or SaTU tests will usually flag this problem. However, intermittent communications may not be easily identified. If Alarm RSSI data logging was enabled when the inaccuracy occurred this file data can be reviewed to see which sensors did not respond.

If the SaTU test indicates that a change in the environment has caused part of the calibration data to be invalidated, parts of the system must be re-calibrated.

RF interference causes can be very difficult to identify and sometimes require the use of a spectrum analyzer. A review of the diagnostic results for noise flags and noise floor monitoring can be used to identify interference issues.

The location inaccuracy can also be reviewed by collecting a few new calibration samples for the CZone in the area concerned and comparing these new samples to existing calibration data. If one sensor's data is significantly higher or lower, the sensor is faulty or has changed. These samples can be deleted after collection if the collected data indicates sensor failure. In that case the new samples would skew the calibration data and should be discarded. If the new samples are consistent within themselves and different from older samples this indicates an environmental change and recalibration may be required.

If a CMPC error occurs such as improper data save to hard disk or data access error then the Flare database may fail to load properly. This usually results in the alarm being located inaccurately or not at all. Database backup copying and pathname verification should correct this problem. A backup copy of the database should be made on removable media after any recalibration is performed.

4.1.8 Communications Problems

Before diagnosing communications problems it is important to understand IP networking, the communications path, different media and how they are affected. IP networking is beyond the scope of this manual. However, the Network Manager includes diagnostic tools and logs that can be helpful. IP addressing setups should be verified as well as managed network switch settings.

A Parts List

Component	Part Number	Description
Flare Control Equipment and Software		
Bundled computer and software package	T1FG0800	Industrial Windows 7 computer (monitor not included) 00SP2800 and all required Software: Flare T1SW0400 Network Manager Service Suite 00FG0220 Universal Configuration Module 00SW0100 Flare Calibration Tool T1SW1000 programming cables: SU GE0444 (UCM interface cable, connects PC running UCM to SU) PPD T1EM1800 (adapter cable for connecting UCM to PPD)
Flare database	T1SW0900	Flare database with map files and defined PZones and CZones (does not include calibration)
22 in. monitor	00SP2313	22 in. wide screen monitor (115/230 VAC)
24 in. monitor	00SP2314	24 in. wide screen monitor (115/230 VAC)
27 in. monitor	00SP2315	27 in. wide screen monitor (115/230 VAC)
Flare Sensor Unit		
Sensor Unit	T1EM1700	Flare Sensor Unit (SU) receiver and plastic enclosure (unit can be configured to function as a sensor and test unit)
SU replacement card	T1BA1700	Sensor Unit circuit card assembly
Flare Personal Protection Device		
PPD with leather holster	T1FG1601	Flare portable personal protection device alarm transmitter
Fixed-position FPD	T1EM0400-002	Flare fixed-position alarm transmitter
Flare accessories		
Straight-in cable entry	T1KT0701	Straight-in cable entry gland (50 pcs)
90º cable entry	T1KT0702	90º cable entry gland (50 pcs) (enclosure hole must be enlarged to fit)
Bulkhead TNCs	T0884	bulkhead TNC-F to TNC-F
Security screws (PPD)	T1KT0402	Security screws for PPD housing (60 pcs) requires T8 bit

Component	**Part Number**	**Description**
Security screws (PPD)	T1KT0403	Security screws for PPD battery cover (40 pcs) requires T10 bit
Security screws (SU)	T1KT0800	Security screws for SU enclosure cover (60 pcs) requires T8 bit
Security screw bit	GX0315-T10	T10 security screw bit (for PPD battery cover)
Security screw bit	GX0315-T8	T8 security screw bit (for SU enclosure cover and PPD housing)
Leather holster	T1SP0300	Replacement holster for PPD
Rubber whip antenna kit	T1KT1100	Rubber whip antenna kit for mounting external antennas on SU enclosure
Antenna extender kit	T1KT0300	Antenna extender kit for mounting rubber whip antennas up to 15.25 m (50 ft.) away from the sensor unit
Yagi antenna kit	T1KT1102	Yagi antenna kit for mounting an antenna outdoors up to 16.5 m (55 ft.) away from the sensor unit
Omni antenna kit	T1KT1104	Omni antenna kit for mounting an antenna outdoors up to 16.5 m (55 ft.) away from the sensor unit
Network accessories		
PoE switch	T1SP1201	24 port managed class 3 PoE switch
Fiber optic switch	T1SP1202	24 port gigabit fiber optic switch
Fiber SFP module	GE0510	Fiber SFP module, 2 per link between T1SP1201 and T1SP1202

B Specifications

Sensor Unit	**Power consumption**	• 1.2 W maximum (25 mA)
	Powering requirements	• Power over Ethernet - PoE Class 3 switch
	Environmental	• Indoor installation: • Temperature -20 to 60º C (-4º to +140º F) • Humidity 10 to 95% non-condensing
	Enclosure dimensions (including mounting flanges) **Enclosure cover**	• L x W x H 25.4 x 14.8 x 5.6 cm (10 x 5.8 x 2.2 in.) • Surface mounting holes 4 x 4.75 mm (4 X 3/16 in.) 2 keyhole slots (4.75 mm) • L X W 22.2 X 14.6 cm (8.7 X 5.7 in.)
	Wiring connections	• RJ-45 Ethernet (Category-5e cable) • USB
	Operating Frequency Range	• 450 to 470 MHz • dual frequency alarm transmission can be enabled at sites where 2 frequencies are available
	Onboard antennas	• Two orthogonal PCB IFA antennas

Personal Protection Device	**Power consumption**	• Minimum one year battery life (with three test transmissions per day) • Automatic low-battery alert transmission (minimum 15 day battery life after the first low battery alert)
	Power source	• 9-V alkaline battery
	Environmental	• Temperature -20º to 60º C (-4 to 140º F) • Humidity 0 to 99% non-condensing
	Dimensions	• 12 L X 5 W X 2.5 D cm (4.7 X 2 X 1 in.)
	Wiring connections (cable port)	• Pull-pin (user-selectable tamper activation) • USB adapter cable (UCM interface cable for PPD configuration)
	Operating frequency range	• 450 to 470 MHz (configurable for local regulations) • dual frequency alarm transmission can be enabled at sites where 2 frequencies are available
	Transmission range	• 1 km (0.6 mile) line of sight (100% coverage within prescribed areas)

Fixed Protection Device	**Power consumption**	• Minimum one year battery life (with three test transmissions per day) • Automatic low-battery alert transmission (minimum 15 day battery life after the first low battery alert)
	Power source	• 9-V alkaline battery
	Environmental	• Temperature -20º to 60º C (-4 to 140º F) • Humidity 0 to 99% non-condensing
	Dimensions	• 13 X 9.4 X 8.9 cm (5.1 X 3.7 X 3.5 in.)
	Wiring connections	• USB adapter cable (UCM interface cable for PPD configuration)
	Operating frequency range	• 450 to 470 MHz (configurable for local regulations)
	Transmission range	• 1 km (0.6 mile) line of sight (100% coverage within prescribed areas)