# Architectural and Engineering Specification for a Security Management System

## StarNet 2™

This document is intended to provide performance specifications and operational requirements for the StarNet 2 Security Management System. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

Senstar, the Senstar logo, FlexZone, OmniTrax and UltraWave are registered trademarks. XField, UltraLink, FiberPatrol, the Senstar LM100, and Silver Network are trademarks of Senstar Corporation. The information in this document is subject to change without notice. Senstar reserves the right to make changes to product design or manufacturing methods, as engineering progresses, or as other circumstances warrant.

# PART 1 GENERAL

## 1.1 System Summary

The contractor shall install a Security Management System (SMS) that manages alarms and events generated by Perimeter Intrusion Detection Systems (PIDS) and integrated security products.

The SMS software shall run on Microsoft Windows operating systems and be designed to manage daily routines and activities as well as crisis situations. It shall enable an organization to reduce its reaction time, improve its efficiency and safeguard its personnel and property.

The user interface shall be optimized for operator efficiency and ease-of-use. The location and coverage area of each security sensor shall be displayed visually on a map. When an alarm occurs, the operator shall be able to quickly determine its location, type, and severity as well as receive alarm-specific procedural information. If any cameras are associated with the sensor, the SMS shall be able to issue instructions to an external Video Management System (VMS).

The SMS shall be optimized to support sensors and software that use Senstar communication protocols. This includes, but is not limited to, the following systems: FlexZone, the Senstar LM100, FiberPatrol, FlexPS, OmniTrax, UltraLink, UltraWave, XField and the Alarm Logic Engine. Third-party security products, connected via dry-contact alarm relays, shall also be supported. Third-party security products may also be integrated in software via the Silver Network protocol.

The SMS shall be designed as an open platform that enables integrations with other systems.

## 1.2 Warranty

The product shall be under warranty for a minimum of two years from the date of purchase.

## 1.3 References

The following acronyms and abbreviations are used in this document:

- GB: Gigabyte
- PDF: Portable Document Format
- PC: Personal Computer
- PIDS: Perimeter Instruction Detection System
- SMS: Security Management System
- SQL: Structured Query Language
- VMS: Video Management System

# PART 2 PRODUCTS

## 2.1 Security Management System

A. The contractor shall supply a Security Management System (SMS).

B. The SMS shall monitor, display, and manage alarms and events generated by Perimeter Intrusion Detection Systems (PIDS).

C. The SMS shall be able to manage other security products when integrated with the site's PIDS.

## 2.2 Manufacturers

A. The StarNet 2™ Security Management System from Senstar Corporation (www.senstar.com) meets the requirements stated in this document.

## 2.3 Architecture and Network Requirements

A. The SMS shall use a 3-tier client/server/database architecture that uses off-the-shelf hardware and software, provides subsystem isolation, and simplifies maintenance and upgrades.

B. The SMS shall be scalable in size, ranging from a single workstation combining the client, server, and database, to a dedicated server with workstations in different physical locations.

C. The SMS shall be future-proof, in that it runs on off-the-shelf, upgradable PC hardware, uses the Windows operating system, and supports industry-standard IT policies and procedures.

D. The SMS shall support industry-standard IT processes for the backup of alarm and event data as well as sensor configurations.

## 2.4 Hardware and Operating System Requirements

A. Application server:

1. The application server shall be compatible with the following operating systems:

   a. Microsoft Windows 7 Professional (32-bit or 64-bit)

   b. Windows 10

   c. Microsoft Server 2008 R2

   d. Microsoft Server 2012

   e. Microsoft Server 2016

B. Client workstation:

1. The client application shall be compatible with the following operating systems:

   a. Microsoft Windows 7 Professional (32-bit or 64-bit)

   b. Windows 10

c. Microsoft Server 2008 R2

d. Microsoft Server 2012

e. Microsoft Server 2016

2. Up to 100 workstations shall be supported per deployment.

3. The client workstation's hardware specifications shall be met by an off-the-shelf professional workstation that meets the following minimum specifications: i5 processor, 8 GB RAM, and a 1080p display.

4. The client workstation shall support input from a keyboard and mouse.

5. The client application shall support common computer monitor display aspect ratios, including widescreen (16:9).

6. The client application shall be designed to run-full-screen to prevent inadvertent or unauthorized manipulation of application windows.

C. Database:

1. The system shall store its sensor and configuration data in a Microsoft SQL database. The application shall support:

a. Microsoft SQL Server 2008 R2 Express

b. Microsoft SQL Server 2008 R2 Standard

c. Microsoft SQL Server 2014 (included with system)

d. Microsoft SQL Server 2016

## *2.5* Features

A. The system shall support the following features:

1. Centralized or distributed management of at least 10,000 intrusion detection sensor input points.

2. Integration of alarms and geographical maps in an easy-to-use graphical interface. Each configured sensor shall be able to represent a geographical location and coverage area.

3. Geographical, tabular, visual, iconic, and audible representations of alarms

4. Ability to issue commands to third-party video surveillance and recording systems. The system shall support both manual and automatic issuance of camera and video control commands.

5. Alarm prioritization, sorting, filtering, and assigning

6. Alarm escalation (rule triggering if an alarm is unacknowledged or not reset after a configured amount of time)

7. A rule engine service that can perform automatic actions based on status or manual changes.

8. User interface controllable by keyboard and mouse.

9. Graphical, point-and-click configuration of security sensors. Perimeter sensors shall be configured by drawing lines on the map to indicate their coverage area.
10. Centralized user management and access control with at least 4 types of users, each of which having a different and customizable set of permissions.
11. Report generation (user activity, alarms/events, and status).
12. On-screen display of alarm and scheduled-based operator procedures.
13. On-screen display of the active state of a sensor (alarm, secure, tamper, fault, or disconnected).

## 2.6 Capabilities

A. The system shall provide real-time situational awareness of the status of the perimeter and intrusion detection sensors.

1. Maps: The system shall graphically depict the sensors and alarms onto a set of custom geographic or spatial maps.
    a. The system shall enable the facility owner to import their own JPEG (.jpg) images for use as maps.
    b. The system shall support at least 128 individual maps. Using the maps as a visual guide, the system administration shall be able to add sensors using a point-and-click interface in order to represent their real-world locations and coverage.
    c. Workstation-specific maps: The system shall enable specific maps to be assigned to individual workstations
2. Alarm monitoring and notifications:
    a. The system shall support the monitoring of a minimum of 10,000 sensor input points.
    b. Alarms shall be indicated on the workstation in a combination of ways: geographical position on a map, tabular, visual, iconic, and audio. For perimeter alarms, the entire coverage area line shall flash and ranging information displayed, if supported.
    c. The system shall support a 2-stage alarm process where alarms are first acknowledged, then closed when the cause is resolved.
    d. Individual alarms shall be routable to specific workstations.
    e. Sorting: The operator shall be able to sort alarms by different criteria, including time, type, station, and priority.
    f. Filtering: The operator shall be able to limit the display of alarms to just those that apply to his or her workstation, if enabled by the systems configuration.

g. Processing: The operator shall be able to acknowledge an alarm and take the necessary action. Upon securing the alarm, the alarm shall be closed and the reason recorded.

h. Auto-processing: The system shall provide a configurable auto-acknowledge function where alarms are automatically acknowledged and/or reset.

i. Forwarding: The operator shall be able to forward alarms to other workstations for processing in multi-workstation environments.

j. Escalation: The system shall be able to trigger a rule if an alam is not unacknowledged or not reset by an operator after a configured amount of time.

k. Type: The system shall differentiate between sensor alarms, tamper alarms, (e.g. enclosure open), and diagnostic alarms (e.g. system failures or maintenance).

l. Masking: The system shall enable operators to:

.1 Temporarily disable or mask an alarm, if the permission is enabled in the system's configuration.

.2 Mask an alarm permanently until an operator unmasked it, if the permission is enabled in the system's configuration.

m. If an equipment failure causes a sensor or zone to go offline (partially or fully), the system shall indicate the affected area.

n. Emails: The system shall provide the option of auto-generating and sending of email messages in response to alarms.

o. Color and symbol: The system shall use a system of color codes and symbols indicate the nature and type of an alarm.

3. Video integration:

a. The system shall enable manual or automatic video controls in response to alarms.

b. The system shall enable pre-programmed video procedures in response to alarms.

c. The system shall be able to generate custom ASCII text strings in response alarms.

4. Network status:

a. The system shall provide a visual summary of the current state of the sensor network, the database, and security subsystems.

5. Response procedures:

a. The system shall display on-screen procedures and tasks for each type of routine or emergency event.

B. Alarm procedure management:

1. The system shall provide alarm-specific procedures (checklists) for operators.
2. Procedures shall be centrally managed by system administrators.

C. Note management:

1. The system shall enable operators to record time-stamped typed notes into the system to record observations or other concerns as they related to specific alarms.

D. Auditing and reporting:

1. The system shall enable reports to be generated in the following formats: on-screen, Portable Document Format (.pdf), and Excel-compatible comma-separated values (.csv).
2. The system shall maintain a history of alarms and user events.
3. The system shall generate the following reports:
    a. Audit: View the activity, actions, response time, and received events for each user over a selected period of time.
    b. Events: View the generated events over a selected period of time, including the sensors involved, the time and duration, the location, resolution reasons, notes, and any performed tasks.
    c. Sensors: View the status of each sensor over a selected period of time.

E. Security and access control:

1. The system shall limit access to configuration and operation functions according to a client workstation's IP address.
2. The system shall provide user access control through the use of user accounts, passwords, groups, and permissions.
3. The system shall support user authentication.
4. User accounts and group privileges shall be centrally managed from an administration account.
5. User Groups shall have configurable permissions to enable organization to customize them according to their own requirements.

F. System configuration

1. Sensor configuration:
    a. The system shall receive status and state information from the security sensors whereby events and output points can be monitored and managed.
    b. The system shall enable system administrators to configure the placement and display of alarm sensors using a graphical, select-and-place interface.
    c. The coverage area of perimeter sensors shall be configured by drawing multi-segment lines on the map. For sensors with ranging capabilities, the system shall enable the operator to configure its ranging values.

d. The system shall provide the option to enable and disable sensors based on a schedule.

e. Each sensor shall receive a priority level to assist operators in prioritizing and sorting alarms.

f. The system shall enable alarms to be generated based on defined conditions.

2. Image/map management:

a. The system shall enable system administrators to upload custom images (.jpg) to use as maps by the system. The maps will be used for both the placement of sensors as well as the display of active alarms for the operators.

3. Network configuration:

a. The system shall enable the system administrators to centrally manage access to the following components: database, client workstations, and sensor network.

4. Importing and exporting:

a. The system shall support a means to import an existing configuration or export the current configuration for backup or deployment purposes.

G. Localization:

1. The system shall provide the option for operators to dynamically switch between languages in multi-lingual environments.

2. Supported languages shall include English, French, Spanish, and Russian.

H. Customizable user interface:

1. The system shall enable the customer to provide custom sensor maps and audio notifications.

2. Screen and audio output shall be directable, via PC hardware, to other devices.

### 2.7 System Integration

A. The SMS shall support integration with sensors using the Silver, FiberPatrol, and CCC protocols.

B. The system shall have the capability to be integrated with the facility owner’s new or existing intrusion detection systems.

C. The system shall have the capability to issue commands to third-party video surveillance and recording systems.

D. The system shall enable a deployment to be pre-configured off-site, so that the SMS software can become fully functional after installation with minimal on-site configuration.

E. The SMS shall be able to manage, monitor and control third-party security equipment via their SDK/API

# PART 3 EXECUTION

## 3.1 System Installation

A. The system shall be installed in accordance with the manufacturer’s recommended procedures as defined in the manufacturer’s documentation for the system.

## 3.2 System Configuration

A. The system shall be configured in accordance with the manufacturer’s recommended procedures as defined in the documentation for the system. If bundled with an intrusion detection system, the system may be configured prior to delivery and installation.

## 3.3 User Documentation

A. The supplier shall provide user documentation that explains how to install, configure, operate and maintain the software.

## 3.4 Training

A. The supplier shall provide training materials that provide instruction in the installation, configuration, and operation of the system.

B. The supplier shall offer professional training services to assist the organization in meeting their training requirements.