Architectural & Engineering Specification for

Microphonic Cable Fence Disturbance Sensor (multiplex version)

Purpose of document

This document is intended to provide performance specifications and operational requirements for the Intelli-FLEX™ multiplex version microphonic cable fence disturbance sensor. It is written in a generic format without referring to the Intelli-FLEX system by name or by specific identifiers. These specifications may be copied verbatim to form a generic procurement specification for a microphonic cable fence disturbance sensor.

Classification of equipment

The Intelli-FLEX system is a microphonic cable fence disturbance sensor, used in conjunction with fences, for outdoor perimeter intrusion detection. The Intelli-FLEX system multiplex version functions as an integral component of a centralized control and maintenance facility.

Disclaimer

Contents

1.0 General performance specifications 4

2.0 Signal processor specifications 7

3.0 Centralized control & maintenance.....10

4.0 System installation and commissioning.....10

5.0 System maintenance and repair.....10

6.0 Product certifications.....11

7.0 System availability 12

APPENDIX A: Sennet central controller 13

3.0 Centralized control & maintenance.....13

APPENDIX B: StarNeT 1000 central controller.....19

3.0 Centralized control 19

1.0 General performance specifications

1.1 System description

The microphonic cable fence disturbance sensor shall function as an electronic perimeter intrusion detector. The system shall be used in conjunction with fences to protect the perimeter of a site. The system shall consist of an ultraviolet resistant triboelectric transducer cable, and a microprocessor based dual zone signal processor. The system shall be capable of monitoring different styles of metal fabric fencing such as chain-link, expanded-metal or welded-mesh fence. The sensor shall detect intruders by utilizing signals generated by the minute vibration of the triboelectric transducer cable, caused by attempting to cut, climb, or raise the fence fabric. The system shall be capable of functioning as an integral part of a centralized control and maintenance facility.

When a central controller is used as the primary operator interface, it shall monitor and control the performance of the entire fence sensor system including auxiliary sensors from a centralized location. An operator shall be capable of controlling the system using a color graphics display, a mouse, a keyboard, or an optional touch screen. An optional site map shall be available to display the site-specific features of the system. The central controller shall be capable of acknowledging, processing and reporting alarms. Routine maintenance including diagnostic testing and remote programming of detection parameters shall be available through the central controller.

1.2 System technology

The signal processor shall analyze the signals from the triboelectric transducer cable and shall detect minute vibrations in the fabric of the fence. The processor shall utilize adaptive algorithms, ambient signal compensation and selectable common-mode rejection, to discriminate between actual, false and nuisance alarms, without lowering the probability of detection. The processor shall identify, by type, a cut intrusion and a climb intrusion. The sensor shall have independent adjustments and thresholds for each type of intrusion and shall have the capability to completely mask climb or cut alarms.

1.2.1 Microphonic cable

The transducer shall be an ultraviolet resistant triboelectric sensor cable and shall be attached to the fence by means of ultraviolet resistant cable ties. The cable shall generate signals when an attempt is made to cut, climb, or lift the fence fabric.

1.2.2 Signal processing algorithms

The system shall utilize digital signal processing techniques that employ adaptive algorithms, capable of adapting to specific fence types and environmental conditions.

1.3 Detection properties

1.3.1 Detection sensitivity

The system shall detect intruders climbing, lifting or cutting the fence while rejecting other environmental stimuli. The sensitivity level shall be adjustable for each zone's specific conditions.

1.3.2 Probability of detection

The probability of detection (PD) of an intruder cutting the fence, and for unaided climbing attempts shall be 95% with a 95% confidence factor.

1.3.3 False and nuisance alarms

1.3.3.1 System-generated alarms (False alarms)

The maximum rate for alarms generated by internal electronic processes (cables excluded) shall be less than one per zone per year, averaged over the total number of zones in the system.

1.3.3.2 Environmental alarms (Nuisance alarms)

The system shall operate within specification in typical outdoor environments. The system shall be installed in accordance with the manufacturer's recommendations to minimize the probability of alarms from the following factors while maintaining the full PD for valid intruders:

- precipitation including rain, snow, hail and fog
- sunrise/sunset
- wind
- temperature changes
- sandstorms
- motion of nearby objects (vehicles, etc.)
- motion of surface or underground water
- nearby vegetation up to 30 cm (1 ft.) high
- nearby sources of radio-frequencies and electro-magnetic interference
- seismic vibration
- acoustic or magnetic effects

1.3.3.3 Notification of environmental concerns

Before installation begins, the installer shall alert the customer, in writing, as to all site-specific conditions that may contribute to a higher environmental alarm rate. The customer shall decide whether to remedy the situation or to accept the nuisance alarm sources without any further responsibility on the part of the installer or the manufacturer.

1.4 Sensor characteristics

1.4.1 Zone length

The maximum length of each zone shall be 305 m (1000 ft.) of sensor cable. Individual zone length shall be determined by the physical boundaries of each zone. The sensor cable shall be supplied in rolls of 305 m (1000 ft.) and shall be cut to the correct length at the time of installation.

1.4.2 Fence height

For regular chain-link (i.e. not vinyl-coated), welded-mesh, palisade, barbwire, and concertina fences the following requirements shall apply:

- For fence heights up to 2.5 m (8 ft.) high, a single cable, attached at the midpoint of the fence, shall be adequate for intruder detection.
- For fence heights between 2.5 m (8 ft.) and 4.0 m (15 ft.), the cable shall be deployed in a double pass, with the cables spaced evenly from each other and the top and bottom of the fence.
- For fence heights greater than 4.0 m (15 ft.), the cable shall be deployed in a triple pass with the cables spaced evenly from each other and the top and bottom of the fence.

Depending on the height and type of fence, and the level of security required, it may be necessary to increase the number of cable passes.

1.4.3 Gates

The sensor shall be capable of monitoring or bypassing swinging and sliding gates by using a Gate Bypass Module. The system shall be capable of placing monitored gates in access mode (no alarm when the gate is used), or secure mode within a secure zone, by either local or remote command. The status of the gate (secure or access) shall be reported to the central controller by multiplexed communications.

1.4.4 Conduit

It shall be possible to install the sensor cable inside conduit that has been firmly attached to the fence. There shall be no lowering of the PD, or increase in the rate of false/nuisance alarms, when using conduit that is installed in accordance with manufacturer’s recommendations.

1.4.5 Armor cable

The sensor cable shall be available encased in an armor jacket, for use in areas that have a high potential of physical damage to the cable. Armored cable shall be available in rolls of 100 m (330 ft.) or greater. The armored cable shall be capable of having multiple sections spliced together to the maximum zone length of 305 m (1000 ft.). The spliced cable shall meet all specifications without lowering the PD, or increasing the rate of false/nuisance alarms.

1.5 Performance history

1.5.1 Previous installations

The system shall have been installed in at least ten similar configurations. A list of these projects shall be available.

1.5.2 Customer references

The vendor shall submit the names and telephone numbers of at least four users who shall serve as references for the satisfactory performance of the equipment. The users shall have a minimum of one year's performance experience with the equipment.

2.0 Signal processor specifications

2.1 Signal processor description

Each signal processor shall be capable of monitoring two detection zones. The processor shall operate as a network unit and shall be an integral component of a centralized control and maintenance facility. The processor shall be used in conjunction with a PC based central controller, or a microprocessor based loop controller and shall be capable of providing multiplexed communications via twisted pair copper cable on an RS-485 network or via fiber-optic cable. The processor shall include internal circuitry to protect against lightning and voltage transients.

2.2 Signal processor operation

2.2.1 Distributed processing

The signal processors distributed along the perimeter shall receive and process the signals from the sensor cables while providing fail-safe operation. The failure of one processor shall not affect the signal processing of the other processors along the perimeter.

2.2.2 Total sensor cable length

Total sensor cable length shall be expandable from the 610 m (2000 ft.) maximum using one signal processor to an unlimited length using multiple processors. The detection zone shall be continuous and uniform, and there shall be no gap between the individual zones, when installed in accordance with the manufacturer's recommendations.

2.2.3 Alarm outputs

The signal processor shall identify intrusion, fail, and tamper alarms to a central controller via multiplexed communications.

Alarms caused by climbing, cutting, or otherwise disturbing the fence fabric shall be identified as intrusion alarms. Intrusion alarms shall be distinguished from supervisory alarms.

Alarms caused by power failure, low input voltage, cable fault, or internal electronic fault shall be identified as supervisory alarms. Supervisory alarms shall be distinguished from intrusion alarms.

Alarms caused by opening the outer enclosure shall be identified as tamper alarms. Tamper alarms shall be identified as supervisory alarms.

2.2.4 Self-test

The signal processor shall be capable of self-test by local or remote activation. The self-test will simulate both climb and cut intrusions to fully test the sensor circuitry, including the cables.

2.3 Auxiliary sensor interface

Each network signal processor shall be capable of collecting and transmitting a minimum of two contact-closure events to the central controller, through an internal interface. The interface shall provide at least two relay output points to initiate a self-test of the auxiliary sensors, or to activate other external devices.

2.4 Environmental operating range

The system shall operate within specifications under the following environmental conditions:

- temperatures between -40° C (-40° F) and 70° C (158° F)
- relative humidity between 0 and 95%, non-condensing

2.5 Powering requirements

The processor shall operate at 12 VDC, and shall accept input power from DC power supplies at:

- 12 to 15 VDC, for individual unit powering
  The individual unit DC power supplies shall accept AC power at 115 V, 60 Hz or 230 V, 50 Hz
- 18 VDC to 56 VDC, for network unit powering
  The network unit DC power supplies shall accept AC power from 85 V to 250 V, 50 to 60 Hz

2.6 Reliability/maintainability

The signal processor shall have a mean time between failures (MTBF) of greater than 40 000 hours and a mean time to replace (MTTR) of less than 10 minutes.

2.7 Physical installation criteria

When installed outdoors, the signal processor shall be installed in a weatherproof, painted steel NEMA 4 enclosure, which meets standard IP 66. A stainless steel NEMA 4 rated enclosure shall be available as an option. The enclosure shall include a hinged cover, stainless steel hardware and a tamper device. The enclosure shall be mounted on a pole, separate from the fence on which the sensor cables are mounted, on the secure side of the perimeter. Each processor shall include a suitable ground rod, which is connected to earth ground.

2.8 Sensor calibration

Each sensor zone shall be capable of being calibrated from its respective signal processor. Sensor calibration shall be made using a configuration module, which shall allow the technician to adjust and monitor the response of each zone. The configuration module shall be detachable via a snap-in connector and shall be capable of calibrating each of the processors in the system. The configuration module shall receive power from the processor and shall not require batteries, calibration or maintenance. Accessing the snap-in connector shall require the opening of the processor's enclosure. This action shall cause a tamper alarm to be generated.

2.8.1 Calibration parameters

The following system parameters shall be adjustable by the user:

- **Cut detection**: independent threshold, count and time per zone
- **Climb detection**: independent threshold, duration and time per zone
- **Preamp gain**: to match the fence to the sensor

2.8.2 Restricted calibration parameters

The following system parameters shall be adjustable by a trained technician through the use of a restricted pass-code. These parameters shall only require adjustment for highly-specialized applications:

- **Ambient compensation**: enable/disable, level (for background effects)
- **Common mode rejection**: enable/disable (for environmental effects)
- **Peak trigger value**: (to identify intrusion over background)
- **Cut profile value**: (to better define a cut event over environmental effects)
- **Alarm output relay activation time**: between 0.5 s and 5.0 s

2.9 Audio Module

An optional audio module shall be available to allow an operator to listen to fence noise to assess possible intrusions. The system shall allow audio monitoring of each zone separately or any combination of zones over a twisted-pair audio cable.

2.10 Weather station

An optional weather station shall be available to monitor weather conditions at the site and to supply the data to the signal processor. The processor shall utilize the data to increase the level of discrimination between environmental effects and actual intrusion attempts.

3.0 Centralized control & maintenance

The microphonic cable fence disturbance sensor shall be capable of being integrated into a centralized control and maintenance facility. There shall be 2 options available to use this feature of the system:

- If the centralized control and maintenance feature uses the Sennet® central controller, insert Appendix A into Section 3.0.
- If the centralized control feature uses the StarNeT™ 1000 central controller, insert Appendix B into Section 3.0.

4.0 System installation and commissioning

The system shall be installed and commissioned in accordance with the manufacturer's recommended procedures as defined in the product's installation and setup guides.

Prior to installation, the installer shall have completed a manufacturer's training program and be certified by the manufacturer. Alternatively, the installer shall be required to have the manufacturer, or their designate, provide qualified technical support for installation and commissioning.

Acceptance tests shall be performed in accordance with standard procedures available from the manufacturer.

5.0 System maintenance and repair

5.1 Recalibration requirements

There shall be no need to recalibrate the system after initial calibration except as the fence condition deteriorates (loose fence elements or wires).

5.2 Sensor cable repair

If the sensor cable is cut or damaged, it shall be capable of being repaired using additional cable, if required, and an appropriate splice kit. The splice kit shall require the use of only standard tools (i.e. slot screwdriver, wire strippers, wire cutters).

5.3 Product support

The product shall carry a minimum one-year warranty from the date of purchase.

The supplier shall warrant that the product shall be supported by spare parts and assemblies for a minimum of 10 years.

6.0 Product certifications

The product shall be manufactured in accordance with ISO 9002 standards.

For European installations, the product shall bear the CE mark.

7.0 System availability

A product that meets or exceeds this specification is the Intelli-FLEX™ microphonic cable fence disturbance sensor, available from:

Senstar Corporation
119 John Cavanaugh Drive
Carp, Ontario
Canada K0A 1L0
Telephone: (613) 839-5572
Fax: (613) 839-5830
Toll Free: 800 390-5796 – Canada
Toll Free: 800 676-3300 – US

www.senstar.com
info@senstar.com

APPENDIX A: Sennet central controller

3.0 Centralized control & maintenance

The microphonic cable fence disturbance sensor shall be capable of being integrated into a centralized control and maintenance facility. The central controller shall be PC based with separate operator, supervisor and maintenance interfaces provided via proprietary software. The controller shall provide or perform the following functions:

- Monitor and control the entire security system from a central location.
- Display any sensor alarm condition within 0.5 sec. of the event.
- A default database that includes two site maps.
- An optional custom database that includes customized site maps, secondary language and unique site-specific features.
- The creation of site databases and the display of site maps.
- Simple, menu driven alarm response functions.
- The remote calibration of thresholds for individual electronic components.
- Upgradable software for new version releases.
- Relay contact outputs.
- The control of a video switcher via optional hardware and software.
- The display of sensor system diagnostic test results.
- System expansion and the addition of components.
- Support the optional audio module function.

3.1 Central controller

The central controller shall be based on a real-time multitasking operating system using a PC platform. The operating system shall have deterministic performance whereby the system shall respond to events within a guaranteed time period (0.5 sec.). The system shall be compatible with standard PC hardware systems up to Pentium® processors.

3.2 Operator interface

The standard operator interfaces shall be a color monitor, mouse and keyboard. A touch screen monitor shall be available as an optional interface.

3.3 Central controller capacity

The central controller shall be capable of supporting a minimum of 62 network compatible devices including microphonic cable fence disturbance signal processors.

3.3.1 Input point capacity

The central controller shall be capable of collecting a minimum of 248 input points. The actual number of input points shall be determined by the capacity of the input devices used in the system and the number of states for each device. Each input point shall be capable of supporting supervised inputs with 3 states (alarm, tamper, secure).

3.3.2 Output point capacity

The central controller shall be capable of distributing a minimum of 2 outputs per microphonic cable fence disturbance signal processor to a maximum of 124 points. The actual number of output points shall be determined by the capacity of the output devices used in the system.

3.3.3 Optional I/O components

Optional network compatible devices shall be available to utilize the I/O capacity of the central controller. These devices shall be available in the following configurations: 16 inputs/8 outputs, 64 inputs/32 outputs, 64 inputs/64 outputs expandable to 256 inputs/256 outputs in groups of 64.

3.4 Display capability

The central controller shall be capable of displaying alarms either on two default system maps, or on optional site-specific maps. Each map shall display the signal processors, the sensor zones, the auxiliary sensors and the status of the associated zones.

3.5 Central controller operating description

The central controller shall be capable of annunciating alarm conditions using four distinct methods: local audible indication, visual indication, relay contact closure and through a serial communications port (requires optional hardware and software components).

3.5.1 Audible alarm indication

The central controller shall be capable of annunciating alarm conditions in any zone by generating an audible signal through the standard PC speaker or buzzer. The signal shall continue until an operator acknowledges the alarm.

3.5.2 Visual alarm indication

The central controller's VGA monitor shall be capable of displaying a visual indication of alarms on a graphical representation of the system or site. The display shall indicate the zone location and type of each alarm. Each zone of the system shall appear on the display as either a physical line or a symbol. The current state of each zone shall be indicated by the zone's color on the monitor: access (yellow), secure (cyan), alarm (red), and fail (magenta). The alarm display shall remain until an operator acknowledges the alarm.

3.5.3 Operator prompting

Operator response to system alarm activity shall be facilitated by alarm prompt messages.

3.5.3.1 Alarm prompt

During alarm conditions, user-defined zone-specific information shall be displayed on a text line at the bottom of the monitor. The text line shall be a maximum of 70 characters.

3.5.3.2 Location prompt

During alarm conditions, an alarm location message shall be displayed for each zone that is in alarm state. The message shall be field programmable and shall be retained on disk during power-out conditions.

3.5.3.3 Response prompt

During alarm conditions, individual operator response messages shall be displayed in the order that the alarm inputs are received, for each zone that is in alarm state. The messages shall be field programmable and shall be retained on disk during power-out conditions.

3.5.4 Contact-closure output (optional)

The central controller shall be capable of providing voltage-free, contact-closure outputs for alarm response in each zone in the system. The contact-closure output function shall be capable of operating in an automatic mode whereby alarm conditions shall be reset upon the removal of the alarm stimulus, without operator intervention.

3.5.4.1 Optional output type

The central controller shall be capable of providing normally open or normally closed contacts for other integrated systems through the use of transponder units.

3.5.5 Relay output cards (optional)

The central controller shall be capable of supporting two optional relay output cards to control or drive auxiliary devices. Each relay output card shall provide either 16 or 32 contact closure outputs to the system.

3.5.6 System menus

The central controller shall display user-selectable menus on the screen. The menus shall provide access to specific functions through keyboard, mouse or optional touch screen controls. A separate set of menu screens shall be provided for system operators, supervisors and maintenance personnel. The menus shall provide a graphical user interface to simplify the performance of each system task.

3.5.6.1 Operator menus

Operator processing menus are divided into operator normal processing menus and operator alarm processing menus.

3.5.6.2 Operator normal processing menu

In the operator normal processing menus, the operator shall be able to:

- view a checklist of information
- view site maps
- perform a diagnostic test of all self-testing sensors
- change sensor status to access or secure
- process sensor and supervisory alarms

In systems that include the video switcher option, the operator shall have menu driven access to the camera views, for display on CCTV monitors.

3.5.6.3 Operator alarm processing menu

The system shall automatically switch to the operator alarm-processing menu when an alarm is generated regardless of other system activity. In the alarm-processing mode, the system shall perform the following functions:

- notify the operator that an alarm has occurred by sounding an audible alarm that requires operator acknowledgment
- display on the monitor the type and location of the alarm
- display on the monitor user-defined instructions on how to process the alarm
- return to the pre-alarm state after the alarm has been processed

3.5.6.4 Supervisor menu

In the supervisor-processing menus, the system supervisor shall be able to:

- assign passwords and menu access to individual users
- schedule automatic access for sensor groups and zones
- create a checklist of information
- create location and alarm prompts for display on the monitor
- create a list of alarm causes that shall be used by the operators during alarm processing
- review system activities
- generate statistical reports for equipment and sensors
- create and perform alarm simulation sequences

3.5.6.5 Maintenance menu

In the maintenance processing menus, the system maintenance technician shall be able to:

- produce status and test reports for equipment and sensors
- examine the input/output point assignments
- adjust the detection parameters of the sensors
- access the operating system

3.5.6.6 Setup menu

In the setup processing menus, the system maintenance technician shall be able to:

- verify the display color of the monitor
- align the optional touch screen
- set the system date and time
- change the format of the date
- set the system to automatically transfer alarms that are not processed within the timeout period
- set the maximum time to acknowledge an alarm before a remote alarm is generated
- assign alarm priority levels
- set the system to automatically switch to the highest priority alarm during multiple alarm processing
- set the communication parameters for communication with system devices
- copy site database information from a floppy disk to the system hard disk
- copy site database information from the system hard disk to a floppy disk
- shut down the system

3.6 Datalogging

3.6.1 Hard-copy output capability

The central controller shall be capable of generating a hardcopy record of all system activity by connecting a printer. The record shall include the time, date, details of the event and the operator's response.

3.6.2 Activity log files

The central controller shall maintain an event log of all system activity on the system's hard drive. The capacity of the event log shall be a minimum of 250,000 lines. The central controller shall notify the operator when the event log is at 90%, 95% and 100% capacity.

3.6.3 Serial communications output (optional)

The central controller shall be capable of outputting the status of all sensor zones and auxiliary systems via an RS-232 serial data link (requires optional hardware and software components). The output signal shall use an acknowledged communication protocol to ensure complete and accurate transmission of system messages.

APPENDIX B: StarNeT 1000 central controller

3.0 Centralized control

The microphonic cable fence disturbance sensor shall be capable of being integrated into a centralized control facility. The alarm annunciation, control and communication system shall operate in a Windows-based (Windows NT, 2000, 98SE, ME) operating system using a PC-compatible platform. The system shall allow an operator to control and maintain a site's security system from a central location. Functions shall include perimeter security sensor monitoring, door control, duress and panic monitoring, intercom and CCTV control.

Alarm processing operations shall be performed using a keyboard, mouse, trackball and/or touch screen monitor. All system events, operator actions and maintenance information shall be stored on the computer hard disk to maintain a permanent record of system activity.

The system shall provide the capability of creating site-specific maps and databases that include the equipment and features of individual sites and security systems. The system shall be programmable for the unique alarm response requirements of each individual site. Site information and alarm data shall be displayed on color-coded maps on a high-resolution color monitor.

The alarm signal communications network shall be designed specifically for security monitoring applications. The network shall provide communications between a centralized maintenance and control facility and remote security devices.

The network shall collect signals from the remote security sensors and deliver the signals to the centralized maintenance and control facility via a high-speed serial data link. The network shall deliver test, maintenance, control and alarm response signals from the centralized control and maintenance facility to remote security devices. The network shall support dual redundant data paths over either RS-422 copper wire, or fiber optic cable.

3.1 System architecture

The minimum system architecture for the alarm annunciation and communication system shall include the following components:

- a Network Monitor and Workstation (PC-compatible computer) that includes:
    - a microprocessor (minimum 600 MHz Pentium® III)
    - a minimum of 64 Mb of RAM
    - a floppy disk drive
    - an IDE hard disk drive (minimum 6 GB)
    - a battery-backed calendar clock
    - an AT enhanced keyboard
    - a serial or PS/2 or USB mouse or trackball

- Windows 98SE operating software (NT optional)
- a high-resolution color monitor
- a parallel printer
- an audio card and speakers
- a software package
- an software protection key device

Note: Refer to paragraph 3.1.1 for optional components to the alarm annunciation, control and communication system.

The minimum system architecture for the alarm communications network shall include any combination of the network devices (transponders) described in paragraph 3.1.2. Each network shall have a capacity to accept up to 128 devices.

3.1.1 Optional components

The system shall provide the necessary interface capabilities for the following optional components:

- a touchscreen color monitor
- Ethernet adapters and hubs (10baseT, 100baseT, 100baseT Fiber Optic)
- CCTV video switchers
- Digital video recorders
- multiple workstations for multi-station operation (64 maximum)
- a second system and monitor for supervisory and maintenance use
- port expansion cards for the addition of serial/parallel devices to the system

3.1.2 Network devices

The alarm signal communication network shall be capable of supporting the following network devices to a total of up to 128 devices:

- **Field Transponder units**, acting as intelligent nodes in a distributed architecture monitoring system, collect alarm sensor data and translate the data into network compatible signals. The transponder units also distribute signals from the centralized control and maintenance facility to the sensors and security devices of the network. Each field transponder shall be capable of 8 supervised inputs and either 4 or 8 relay outputs.
- **Local Transponder units** collect, translate and distribute alarm sensor data, and control signals in areas with high concentrations of I/O points. Each local transponder shall be capable of monitoring a maximum of 64 inputs and 64 outputs in a variety of configurations using up to 4 I/O modules as follows:

    - 32 optically isolated switch inputs

- 16 end-of-line resistor supervised sensor inputs (using 32 input points)
- 32 open collector outputs that can be used to operate 32 high current relays
- 16 low current dry contact outputs

The Local Transponder unit shall use an EchoCheck Bus to communicate with the I/O modules. All Local Transponder units and I/O modules shall be rack-mountable in EIA rack mount enclosures.

- **Local graphic panels** provide alarm display and processing functions at remote locations. Each panel shall be capable of displaying and processing 128 LED lamps and supporting 64 momentary switch contact inputs, as well as lamp test, keyclick and Sonalert® functions.
- **Signal processors** from microphonic cable fence disturbance sensor systems, which shall contain the circuitry necessary to monitor the sensor cable detection signals. Each processor shall be capable of protecting two independent alarm zones, each up to 300 m (1,000 ft.) in length. There shall be a maximum of 99 processors per network using the Crossfire protocol.
- **Signal transponders** for bistatic microwave sensor system processors, which contain the circuitry necessary to monitor signals from the microwave field. Each transponder shall be capable of monitoring two independent alarm processors, each with zones up to 183 m (600 ft.) in length. There shall be a maximum of 64 transponders (128 zones) per network using the Crossfire protocol. An acceptable product that meets or exceeds these requirements is the Intelli-WAVE™ system processor.

3.2 System capability

The system shall be available in two distinct configurations for controlling small and large security systems.

3.2.1 Display capability

Each system shall be capable of displaying a limited number of individual map screens depending on available computer memory. Each map shall be capable of displaying a minimum of 255 icons. All control features shall be icon-based for ease of recognition and operation.

3.2.2 Transponders

The **large system** shall support a maximum of 128 Network Devices per network, as described in Section 2.2 above.

The **small system** shall support a maximum of 32 Network Devices per network, as described in Section 2.2 above.

3.2.3 Workstations

It shall be possible to network up to 64 systems/workstations peer-to-peer on a TCP/IP network. Each network device and component shall be assigned a unique address to ensure accurate communications and alarm reporting

functions. Using this global point identification, it shall be possible to monitor and control any I/O point on any workstation from any workstation on the LAN.

3.2.4 Primary device capability

Each system shall provide RS-232 serial ports for connecting the primary sensor and I/O data devices. The system shall support the following primary devices:

- serial interface devices
- alarm communications networks (copper and fiber optic)
- video controllers and switchers
- digital video recorders

3.2.5 Simultaneous operation and maintenance capability

Using a TCP/IP network, the system shall provide the capability of connecting a secondary system with monitor and printer for performing maintenance, diagnostic and supervisory functions without disturbing normal operation.

3.2.6 Input point capability

The large system shall support up to 8192 input points (2048 for the small). The actual number of input points is determined by the primary devices used in the system and by the number of states for each input to the primary devices. Each input point shall represent an alarm/tamper condition of a physical input. Within this specification, an input point is defined as a reporting point on a hardware device that collects data from an associated alarm.

The alarm communications network shall be capable of supporting 8192 input points.

3.2.7 Output point capability

The large system shall support 8192 output points (2048 for the small). The primary devices used in the system determine the actual number of output points. Within this specification, an output point is defined as a physical point on a hardware device that responds to data from an associated input point or display state.

The alarm communications network shall be capable of supporting 8192 output points.

3.2.8 Drive point capability

The system shall provide a minimum of 2 main categories of alarms as described in the following list:

Display alarms are displayed on the site maps when a sensor is activated and/or when a hardware device fails.

Remote alarms are annunciated at a remote location when a sensor is activated and/or when a hardware device fails.

3.2.8.1 Display and remote alarm types

The system shall support a minimum of two distinct alarm types, based on input point state, for the display and remote alarm categories:

Sensor alarms are generated when a sensor detects an alarm condition (e.g., an intrusion).

Tamper alarms are generated when a sensor is physically disturbed.

3.2.8.2 Display states

The system shall support the following display state changes:

Alarm - the display point changes from a secure state to an unacknowledged state. Indicator flashes and a WAV file is played on the sound system output.

Acknowledge - the display point changes from an unacknowledged state to an acknowledged state. Indicator stops flashing and shows steady alarm status. WAV files stop playing on the sound system.

Access - the display point changes from a secure state to an access state.

Secure - the display point changes from an access state to a secure state.

3.2.9 Passwords

There shall be 256 password levels. Each operational activity shall be assigned a password level. Each operator shall be assigned a password level and a password. The operator must have a password level equal to or greater than the password level of an operational activity in order to operate that activity.

3.2.10 Activity archive

The system shall allow a minimum of 100,000 lines of events and actions to be stored on the hard disk in log files by calendar date. The last 8000 events shall be displayed on the monitor in an event window on command. All events may be printed out or saved in a comma-delimited file format for export to another program for analysis.

3.3 Site Creation characteristics

The programming software shall include graphics oriented templates that shall allow a user to customize the system for site-specific applications without factory assistance. The templates shall feature graphical representations of security facilities upon which users enter site-specific information. The user shall be able to import illustrations, digital photos and auto-CAD files as .bmp (bitmap) files to form the basis of site-specific maps. The user shall also be able to associate .Wav files with alarm events. The programming software shall translate the data into binary logic for system use.

The software shall use icons and standard menus in a five-step process to create the site database:

- A site configuration/bitmap shall be imported or created.

- All input and output points on each transponder shall be assigned a unique component address and function

- Each component shall be assigned one or more control icons to identify how it interacts with other components to operate the facility and indicate its status.

- Screen icons are assigned to components and controls in order to allow an operator to control the facility on the display. *.WAV files can be associated with individual zone alarms and/or alarm groups (e.g. duress) for playback during alarm annunciation.

- The setup data is converted into binary logic equations by the program and saved.

3.4 Crossfire Network performance specifications

The alarm communications network shall meet the following general performance specifications:

3.4.1 Communications

The network communications shall be serial duplex with user-selectable baud rate.

3.4.1.1 Error detection

The network shall utilize 16-bit cyclic redundancy check (CRC) to ensure accurate network communications.

3.4.2 Redundant data paths

The network shall be capable of supporting dual redundant data paths. Dual redundant data paths allow network communications to continue in the event that either of the data paths fails.

3.4.3 Unique device addresses

Each network device shall be assigned a unique address to facilitate network communications and to identify the location of alarm conditions.

3.4.4 Network wiring

The Crossfire alarm communications network shall be capable of communicating over either RS-422 twisted pair copper wire or multi-mode fiber optic cable. The RS-422 network shall have a maximum length of 1.2km (¾

mile) between transponders for a maximum loop length of 24.4Km (15.2 miles). The fiber optic network shall have a maximum length of 2km (1.25 miles) between transponders.

3.5 System operating description

3.5.1 Operator alarm processing functions

On alarm, the system shall automatically switch to the map that displays the alarm and the ICON that represents that alarm point will flash. The WAV file assigned to that alarm will play on the computer sound system. The Operator shall have to acknowledge the alarm before processing the alarm.

In operator alarm mode processing, the system shall allow the operator to:

- clear alarm, tamper, and diagnostic alarms
- observe CCTV camera views, individually or in groups, that are associated with an alarm (requires video switcher option)

3.5.2 Operator normal processing functions

In operator normal mode processing, the system shall allow an operator to:

- view a list of activity information
- view site maps
- perform a test of all testable devices/sensors
- change the state of sensors to access or secure
- review the last 8000 events/actions performed on the system

3.5.3 Maintenance functions

In maintenance processing, the system shall allow the maintenance technician to:

- assign passwords and function access to individual users
- examine the input/output point states
- adjust the sensitivity of the sensors
- access the operating system to diagnose system problems
- align the touch screen (in Windows)
- set the calendar clock's date and time (in Windows)
- change the format of the displayed date (in Windows)
- set the communication parameters for system devices
- shut down the system