

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)

Approved for use through 06/30/2010 OMB 0851-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Rodney	W	Fox	Coeur d'Alene	ID	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention

PREMISES MONITORING SYSTEM

Attorney Docket Number (if applicable)

ILNX-1-1002

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number

☐ Firm or Individual Name

Customer Number

59520

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☒ Yes, applicant qualifies for small entity status under 37 CFR 1.27☐ No**Warning**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/James J. Ruttler/			Date (YYYY-MM-DD)	2009-07-23
First Name	James	Last Name	Ruttler	Registration Number (If appropriate)	56919

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		PREMISES MONITORING SYSTEM		
First Named Inventor/Applicant Name:		Rodney W Fox		
Filer:		James Jeffry Ruttler		
Attorney Docket Number:		ILNX-1-1002		
Filed as Small Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional Application filing fee	2005	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				110

Electronic Acknowledgement Receipt	
EFS ID:	5760484
Application Number:	61228044
International Application Number:	
Confirmation Number:	7876
Title of Invention:	PREMISES MONITORING SYSTEM
First Named Inventor/Applicant Name:	Rodney W Fox
Customer Number:	59520
Filer:	James Jeffry Ruttler
Filer Authorized By:	
Attorney Docket Number:	ILNX-1-1002
Receipt Date:	23-JUL-2009
Filing Date:	
Time Stamp:	17:48:22
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$110
RAM confirmation Number	4019
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Specification	ILNX-1-1002AP.pdf	123783	no	12
			183cdd83e6c40466d4cd4ff8010e7731c0f828ea		
Warnings:					
Information:					
2	Drawings-only black and white line drawings	ILNX-1-1002Figures.pdf	33511	no	2
			be9b9c6059f1bc27e444200a85a9581d24fe99e8		
Warnings:					
Information:					
3	Appendix to the Specification	ILNX-1-1002AppendixA.pdf	174231	no	42
			24c85b9e9ce0da98d7f636d0b69882ea5764d874		
Warnings:					
Information:					
4	Provisional Cover Sheet (SB16)	ILNX-1-1002ProvisionalCoversheet.pdf	1523015	no	3
			d31ef5f9d6367dbc7d72bc044829a8105e17d699		
Warnings:					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	29167	no	2
			791218326f7cbe06177716e112e2118647c5052a		
Warnings:					
Information:					
Total Files Size (in bytes):			1883707		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

5

PREMISES MONITORING SYSTEM

10

INVENTOR
Rodney W Fox

DETAILED DESCRIPTION

[0001] This invention relates generally to computer systems, and more specifically, to a premises monitoring system. Specific details of certain embodiments of the invention are set forth in the following description and in FIGURES 1 and 2 and APPENDIX A to provide a thorough understanding of such embodiments. The present invention may have additional embodiments, may be practiced without one or more of the details described for any particular described embodiment, or may have any detail described for one particular embodiment practiced with any other detail described for another embodiment. Any use of “and” or “or” herein is intended to mean either “and” or “or” or both “and” and “or”.

20

[0002] APPENDIX A provides a specific example of one particular embodiment of the invention disclosed herein.

[0003] In some embodiments, the premises monitoring system uses an existing network connection to dispatch critical information as it occurs. The critical information can include fire or security alarm information, mass notification information, hazardous material storage information, utility disconnect location information, floor plan information, photographic image information, or other similar information. The critical information can be dispatched via email, text message, instant message, a website, or other similar methodology. The system can be used by authorities, management, first

25



30 responders, staff, agencies, or other similar entities. The system can be used in
 residential buildings, commercial buildings, industrial buildings, milling/mining
 facilities, manufacturing/treatment facilities, chemical plants, institutional facilities,
 public buildings, military sites, high rise buildings, campus buildings, hotels/conference
 centers, health care facilities, airports, marinas, clean room facilities, religious facilities,
 35 train/subway facilities, amusement parks, resorts, golf courses, fish hatcheries, agriculture
 facilities, or any other similar building or operation. In some embodiments, the system
 provides enhanced notification as a service to small and medium entities without
 requiring independent acquisition of special equipment. In some embodiments, the
 system may be operated independently by a larger entity.

40 **[0004]** In some embodiments, the system receives a signal, identifies a field
 device, obtains critical information associated with the field device, automatically
 dispatches a text message containing the critical information, and automatically
 dispatches an email having text and/or color graphical images/PDF documents containing
 the critical information, and automatically archives data relating to the signal and
 45 dispatch of the critical information. Accordingly, the system can reduce response time by
 promptly providing critical information to a first responder.

[0005] In some embodiments, the system operates in conjunction with existing
 monitoring services. A Digital Alarm Communicator Transmitter (DACT), or other
 similar device, reporting to a monitoring service is modifiable to alternatively and/or
 50 additionally report a signal to the premises monitoring system disclosed herein. For
 example, a DACT's second account can be enabled to alternatively and/or additionally
 report a signal to the premises monitoring system. Reporting a signal to the premises
 monitoring system can be conducted in accordance with National Fire Protection
 Association (NFPA) standards. The system can be configured to receive the signal as a
 55 "Contact ID" signal or any other industry standard transmission protocol signal. Upon



receiving a signal from the DACT, the system can process the signal and automatically dispatch critical information without disrupting an existing monitoring service.

[0006] In some embodiments, the system dispatches critical information via text message and/or email automatically without operator intervention within a few seconds of receipt of a signal from a DACT (e.g., within approximately 3 seconds). The system can dispatch critical information via Short Message Service (SMS) text messaging, email, instant messaging (IM), such as via AOL or MSN, a website, or via other similar technology. The critical information can be dispatched to a computer, phone, pager, personal digital assistant, internet appliance, electronic book reader, or other similar device. The critical information can include a building location, a room description, a GPS coordinate, a device type (e.g., smoke detector, pull station, etc.), a device condition (e.g., alarm or supervisory), a graphic or a PDF document having a black/white or color graphical floor plan, map, site plan, picture, or other image reflecting an exact device location, a sound bite, voice instructions, a message, personnel contact information, passcode or password information, or any other similar critical information. The critical information may be printed, forwarded, edited, or stored for archival purposes.

[0007] In some embodiments, a graphic or PDF document is obtained, stored, and accessible by the system to dispatch as critical information upon receipt of a signal. A device location can be designated on the graphic or PDF document and additional text information can be included on the graphic or PDF document upon receipt of a signal and based upon information contained within the signal. The content of the PDF document can be magnifiable without distortion, even when significantly magnified, and is defined by a relatively small file size for fast transmission (e.g., approximately 250k-300k for a 20,000 square foot floor plan having 50 devices).

[0008] In some embodiments, the system is configured to receive signals from DACT, RADSCAN ALARMNET 7810, LARSNET RCI3300 AND RCI4000, KELTRON RF7300, radio, IP, or other similar sources. The system is configurable to



receive signals in formats including (1) SESCOA, VERTEX, DCI, FRANKLIN FAST - 3X1, (2) SESCOA - 4X3, (3) RADIONICS HEX - 3X1, MODEM IIIa2 and BFSK, (4)
 85 Old ADEMCO, SILENT KNIGHT SLOW - 3X1, (5) ACRON - 4X1, (6) SILENT KNIGHT, NAPCO - 4X2, (7) CFSK, VFSK, SIA - MODEM, (8) FBI SUPERFAST, SUR-GARD, ADEMCO HI-SPEED, (9) ADEMCO EXPRESS and ADEMCO CONTACT-ID – DTMF, or any other similar format such as direct-connect, distributed multiplexer formats, radio formats, and SIA-compliant formats.

90 [0009] The system is configurable to receive signals via reverse polarity, end-of-line resistors, dry contacts, proprietary tone signals, private line, digital dialers, direct connects (e.g., POTS or fiber), star multiplex, distributed multiplex, coded signals, or any other similar methodology. The system is configurable to receive signals via an analog telephone line, wireless communication, internet communication, ethernet
 95 communication, or some other similar methodology. The system is configurable to support a plurality of simultaneous incoming signals. The system is configurable to prioritize incoming signals, such as according to UL standards. The system is configurable to receive test signals. The system is configurable to group incoming signals, such as to batch a group of low priority signals to provide for more efficient
 100 signal management. The system is configurable to provide a swinger suppression function, such as to filter swinger signals that constantly toggle between normal and off-normal states to a manageable number. The swinger suppression function can allow a first occurrence of a signal, track a most recent occurrence of a signal, and track a number of signals. The system is configurable to suppress, ignore, or auto-acknowledge signals,
 105 such as by a signal type, for a period of time, or during severe weather. The system is configurable to filter incoming signals by account status. The system is configurable to detect any failure in a signal communications link and provide an appropriate alert. In some embodiments, the system includes redundant systems to accept signals in the event of failed communication links or for load balancing. The redundant systems can include



110 automatic updates between systems and cross-acknowledgement functionality. In some
embodiments, the system includes a plurality of systems each configured to receive and
process a certain type of signal (e.g., fire alarm signals, home invasion alarm signals).

[0010] In some embodiments, the system is configurable receive and interpret a
plurality of signals. A signal may be activation of a smoke detector, pull-station, or other
115 similar device. A signal may be failure to receive a check-in. For example, in an assisted
living facility, patients may be required to phone, email, or text a check-in to confirm
good health and mobility. Absence of the check-in within a defined time period can
result in a signal being communicated to the system, which can result in dispatch of
critical information and prompt assistance to patients. A signal can be a device failure or
120 signal communications failure. A signal can be a dispatch failure. A signal can indicate
various statuses such as normal, fault, trouble, alarm, or other similar status.

[0011] In some embodiments, upon receiving a signal, and prior to dispatch, the
system is configurable to provide an audible alert, display an appropriate message, and
print an appropriate message. The system can require user intervention to silence the
125 audible alert or clear the message displayed. The system is configurable to accommodate
a plurality of incoming signals by displaying multiple messages and printing multiple
messages. The printed message can include an alarm indication, an account identifier, a
time and date stamp, a field device identifier, a zone identifier, a customizable account
message, a customizable zone message, a customizable field device message, or any
130 other similar information. The system is also configurable to print an acknowledgement.
The displayed message can include an alarm indication, an account identifier, a time and
date stamp, a field device identifier, a zone identifier, a customizable account message, a
customizable zone message, a customizable field device message, or any other similar
information.

135 [0012] In some embodiments, the system is configurable to retain records of
signals, false alarms, acknowledgements, resolutions, restorations, in/out service setting



changes, clock setting changes, clock failures, editing changes, signal communication failures, dispatches, dispatch failures, login/access attempts, printer failures, or any other similar event, occurrence, or information. Retained records can be printed, displayed, forwarded, edited, saved, filtered, sorted, or any other similar function.

[0013] In some embodiments, the system includes a user interface for maintaining account information (e.g., account number, address, telephone number, number of site locations, monitoring hardware address, transceiver model, connection point, service companies etc.), uploading graphical images (.BMP, .RLE, .GIF, .JPG, .JPEG, .PDF, .WMF, .EMF, .CAD, etc.) such as maps, graphics, pictures, videos, floor plans, site plans, photos of personnel, and other similar images, uploading audio files, defining messages, defining site instructions, defining field devices, defining field device groups or categories, defining field device descriptors, defining field device instructions, defining contact information (e.g. key holder name and phone number), defining passcodes or passwords, defining hazards or hazardous materials, defining recommended response procedures, defining camera or video feeds, defining field device positions relative to graphic images, defining icons relative to graphical images, defining graphical images relative to graphical images such as an hierarchical form (e.g., a street level view can be used to navigate to a room view or even a field device view), defining dispatch methods (e.g. email, text message, instant message, website, etc.), defining dispatch destinations (email accounts, phone numbers, etc.), associating any of the above with device codes to be received within signals, dispatching critical information, reviewing archived information, reviewing reports, or any other similar function. The system can provide for templates to provide for duplication of any of the foregoing. The user interface can provide controls for disabling and enabling field devices, signals, alarms, or other similar function. The user interface can provide access to any system function. The user interface can include password controls for access to various features and



functions. The user interface can be accessible locally or remotely and via a local area network, VPN, web page, or some other methodology.

165 **[0014]** In some embodiments, the system provides for management of critical information for dispatch. The management can include displaying various details of critical information associated with one or more signals prior to or in addition to dispatching the critical information. The critical information can be identified by the device code contained within the signal based upon associations discussed with reference
170 to the user interface above. For example, for a given signal, displayed critical information can include the field device associated with the signal, the nature of, location, time, and date of a signal, account information associated with the signal, site and location information associated with the signal, instructions associated with the signal, contact information associated with the signal, graphical information associated with the
175 signal such as maps, floor plans, photographs, and diagrams, a floor plan having a designation of the signal originating position, audio instructions associated with the signal, recommended response procedures associated with the signal, hazards or hazardous materials associated with the signal, or other similar information. The displayed critical information can be arranged in a tabular manner, tree structure manner,
180 or other similar arrangement. For example, the displayed critical information can be arranged via a basic tab, a map tab, a site tab, a notes tab, a details tab, a historical record tab, or any other similar tab having critical information associated with the signal. The displayed critical information can also include information or links to other field devices, such as those in proximity to the field device triggering the signal. The signal triggering
185 the displayed critical information can be queued, organized, managed, acknowledged, resolved, and any notes or activity can be recorded for archival purposes. The displayed critical information can be manually approved for dispatch or can be automatically dispatched without user intervention.



[0015] In some embodiments, the system receives a signal, retrieves critical information associated with a device code within the signal, determines dispatch methods and destinations, and dispatches the critical information using the dispatch methods to the destinations without operator intervention. For example, upon receiving a signal, the system can retrieve critical information associated with a device code within the signal such as account information, graphical images such as maps, graphics, pictures, videos, floor plans, site plans, and photos of personnel, audio files, messages, site instructions, field device identity, field device type, field device description, field device instructions, field device condition, contact information, passcodes or passwords, hazards or hazardous materials, recommended response procedures, camera or video feeds, field device address, field device GPS coordinates, field device positions relative to graphical images, or any other similar critical information. The critical information can make use of color, such as color-coded field device positions relative to a floor plan. The critical information can make use of custom audio/visual indicators, such as sounds or icons relative to a site map. The critical information can include graphical images that are magnifiable without degradation to approximately 6600%. For further example, upon receiving a signal, the system can retrieve dispatch methods and destinations associated with a device code within the signal such as methods of email, text message, instant message, website, phone call, or the like and destinations of email addresses, text message addresses, instant message addresses, website addresses, and phone numbers. Upon retrieving critical information and determining dispatch methods and destinations, the system can dispatch the critical information using the dispatch methods to the destinations. For example, the system can dispatch an email to an email account, a text message to a phone, or a voice message to a phone each containing all or some of the critical information. The system can provide for redundant backup dispatch operations.

[0016] Any of the critical information, dispatch methods, or dispatch destinations may be added, removed, or changed via the user interface. For example, a



hotel can update the system to include guest email addresses and phone numbers as dispatch destinations upon guest check-in. Alternatively, a business can update the system to include employee email addresses and phone numbers as dispatch destinations upon employment. Also, a shopping center can update the system to include consumer
 220 email addresses and phone numbers as dispatch destinations upon entrance to the shopping center. In one particular embodiment, a kiosk can be used to accept dispatch destinations. In another particular embodiment, a magnetic or radio transmitter card/device can be used to quickly supply dispatch destinations. Further, the critical information can be tailored to specific dispatch destinations. For example, more detailed
 225 critical information can be dispatched to first responders while less detailed information can be dispatched to employees, hotel guests, or consumers.

[0017] In some embodiments, the system is implemented using one or more of the following modules.

[0018] iTRANSLATE. In some embodiments, the iTRANSLATE software
 230 module is configured to receive signals and retrieve critical information associated with device codes contained within the signals. The iTRANSLATE software module is a continuously running background program that utilizes a WINDOWS platform. The iTRANSLATE module is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version of the iTRANSLATE module is fully
 235 integrated to allow for recovery. In the event of a WINDOWS operating system reboot, the iTRANSLATE module automatically restarts and reloads without operator intervention.

[0019] iWATCH. In some embodiments, the iWATCH software module contains critical information and dynamically provides the critical information based
 240 upon device codes contained within the signals. Upon receipt of a signal, the iWATCH module begins an automatic processing sequence to determine the critical information for dispatch. The iWATCH software module is a continuously running background program



utilizing the WINDOWS platform. The iWATCH module is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version of the
245 iWATCH module is fully integrated to allow for recovery. In the event of a WINDOWS operating system reboot, the iWATCH module automatically restarts and reloads without operator intervention.

[0020] iDISPATCH. In some embodiments, the iDISPATCH software module controls dispatches of critical information using dispatch methods to dispatch
250 destinations, such as emails and text messages to computers, phones, and personal digital assistants. The critical information dispatched is tailored to a field device based upon a device code contained within incoming signals. Critical information is quickly and automatically dispatched without operator intervention. The iDISPATCH module dispatches all formats or any combination thereof in single or multiple dispatches in a
255 manner that allows cascade notification of unlimited recipients. The iDISPATCH software module is a continuously running background program utilizing the WINDOWS platform. The iDISPATCH module is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version of the iDISPATCH module is fully integrated to allow for recovery. In the event of a WINDOWS operating system
260 reboot, the iDISPATCH module automatically restarts and reloads without operator intervention.

[0021] iMONITOR. In some embodiments, the iMONITOR software module is configured to monitor and log incoming signals, translations, dispatches, and any other system function. The iMONITOR module records a date and time stamp of signals and
265 the post-translated condition of the signals. The information is recorded for retrieval using the iREPORT software module discussed infra. The iMONITOR software module is a continuously running background program utilizing the WINDOWS platform. The iMONITOR module is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version of the iMONITOR module is fully integrated



270 to allow for recovery. In the event of a WINDOWS operating system reboot, the iMONITOR module automatically restarts and reloads without operator intervention.

[0022] iREPORT. In some embodiments, the iREPORT software module provides historical reporting by field device, field device type, condition, account, date, or other similar criterion. The iREPORT module also provides for reports on dispatches
275 and acknowledgements. A backup version of the iREPORT module is fully integrated to allow for recovery.

[0023] iCONFIGURE. In some embodiments, the iCONFIGURE software module provides configuration functionality. The iCONFIGURE module allows for defining account information, graphical images such as maps, graphics, pictures, videos,
280 floor plans, site plans, and photos of personnel, audio files, messages, site instructions, field device identities, field device types, field device descriptions, field device instructions, field device conditions, contact information, passcodes or passwords, hazards or hazardous materials, recommended response procedures, camera or video feeds, field device addresses, field device GPS coordinates, field device positions relative
285 to graphical images, or any other similar critical information. The iCONFIGURE module allows for manual defining of critical information, importation of critical information, as well as use of templates. The iCONFIGURE module allows for association of a field device with a position on a graphical image such as a floor plan or site map. The iCONFIGURE module allows for association of any critical information with any device
290 code to be received within a signal. The iCONFIGURE module allows for testing of dispatches in a virtual state. Access to the iCONFIGURE module is limited by password.

[0024] iARCHIVE. In some embodiments, the iARCHIVE module automatically stores a record of system transactions to the system archive files.

[0025] In some embodiments, the system is embodied on computer readable
295 media or is operated using a computer or computer system.



[0026] While preferred and alternate embodiments of the invention have been illustrated and described, as noted above, many changes can be made without departing from the spirit and scope of the invention. Accordingly, the scope of the invention is not limited by the disclosure of these preferred and alternate embodiments.

300

59520
CUSTOMER NUMBER

-12-



RUTTLER & LONG PLLC

One Union Square
600 University St. Ste. 1919
Seattle, Washington 98101

206-438-6400
www.ruttlerlong.com

FIGURE 1

100

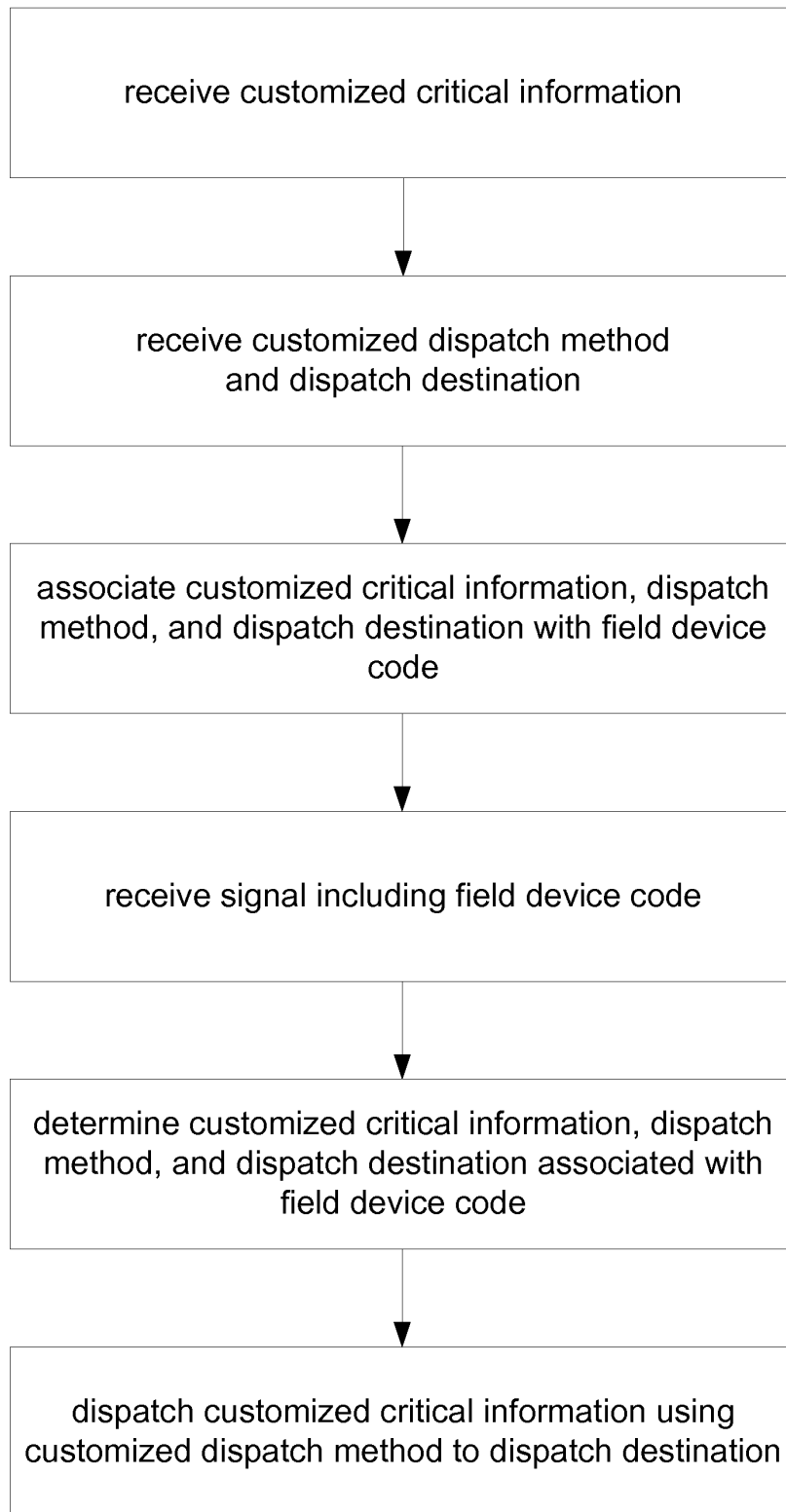
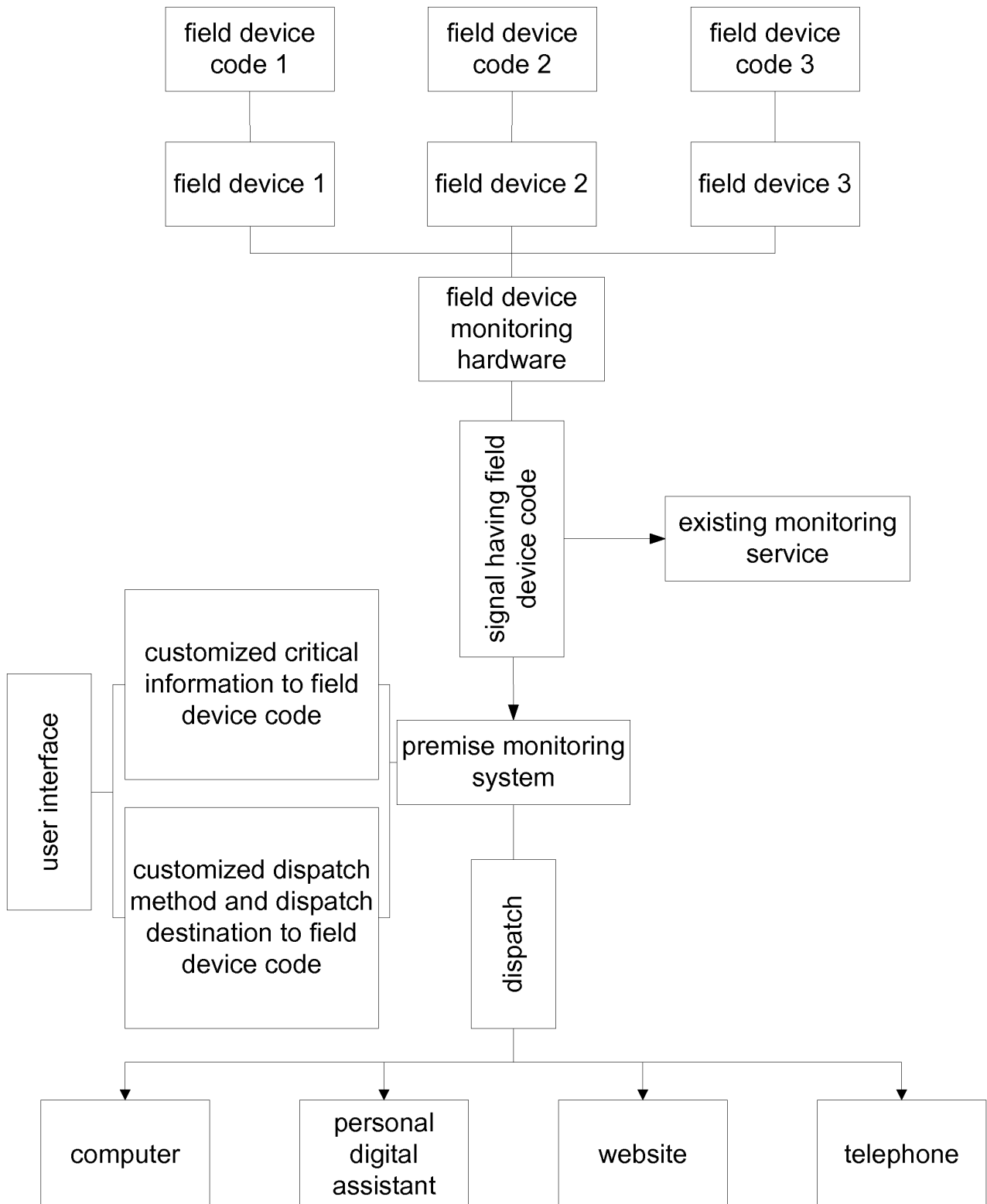


FIGURE 2

200



APPENDIX A

Use your existing network connection and unleash the power to display critical information as it occurs, in real time with just a few simple clicks.

IDEAL FOR AUTHORITIES, MANAGEMENT AND OTHER FIRST RESPONDERS

FIRE/SECURITY ALARMS

MASS NOTIFICATION SIGNALS
HAZARDOUS MATERIAL STORAGE

UTILITY DISCONNECT LOCATIONS

AUTOMATIC EMAIL NOTIFICATION

CELLULAR TEXT MESSAGES

COLORGRAPHIC FLOOR PLANS

PHOTOGRAPHIC IMAGE DISPLAYS

Receive critical information sooner and in greater detail than conventional dispatch...

iLinkx pinpoints the exact device in alarm, automatically dispatching text messages, emails and color graphic images as easily opened pdf attachments, all while automatically archiving the critical data for future reference should it ever become necessary.

iLinkx dramatically reduces response time by providing earlier notification to those first responders needing critical information.

iLinkx pinpoints the exact device in alarm, automatically dispatching text messages, emails and colorgraphic images as simple pdf attachments, all while automatically archiving the critical data for future reference should it ever become necessary.

Receiving industry proven "Contact ID" signals, iLinkx offers a substantial increase in the lifespan and usefulness of your existing equipment investment. Sites that currently have Digital Alarm Communicator Transmitters (DACT's) which report to monitoring services can easily enhance notification with a few minor programming modifications. Operating in an ancillary capacity, in accordance with National Fire Protection Association (NFPA) standards, iLinkx processes information without disruption to the current dispatch procedures of your existing monitoring service.

Interfacing is easy! There are no special hardware or expensive component requirements, nor are there any hidden procedures. Simply subscribe and receive your iLinkx account information, then enable your DACT/s second account (a rarely used feature of existing UL Listed equipment) to also report information to iLinkx and you unleash the power of your internet network.

Experience the benefits of enhanced notification now, placing critical information into the hands of first responders, management, and staff, including those agencies with a need to know.

By connecting to iLinkx you receive critical information in just a few seconds after the signal has been processed. Emails are automatically generated, without any operator intervention, in a standard text format, with such information as

EXAMPLE: Building Location

Room Description

GPS Coordinate

Device Type (Smoke Det. Pull Station, ect.)

Device Condition (Alarm or Supervisory)

Or any other critical information necessary for first responders or thoses with a need to know.

In addition to the text messages, a colorgraphic floor plan reflecting the exact device location is automatically generated, without any operator intervention in an easy to read .pdf attachment. iLinkx colorgraphic images are of the highest quality, with little or no distortion when magnified and can be easily printed, forwarded or stored by the recieipient/s for future reference as needed.

In the past, the creation of high quality colorgraphics required vast amounts of computer file storage space. iLinkx has perfected the process with its patent pending technology that minimizes the actual file size while maintaining the colorgraphic integrity. This allows enhanced notification, in a much shorter time period than conventional technology with a significant reduction in response time.

Additionally, the creation of high quality colorgraphics required very long, computer screen, build times. Again, the patent pending technology further enhanced notification by pinpointing the specific problem area, reflecting the condition on a colorgraphic image that could be printed, forwarded or archived for future reference in as little as a few seconds.

Colorgraphic floor plans, images and layouts that would only work on certain computing equipment are a thing of the past. Imagine, with iLinkx you can unleash the power of your internet network and receive tommorrow's technology, today in an open protocol, non-proprietary, ordanary format. Critical information, automatically generated and dispatched, in a regular email with a common .pdf attachment and no proprietary hardware. Imagine that!

Applications Worldwide

Unleash the power of the internet when every second counts.

iLinkx software services allow small and intermediate size clients an opportunity to subscribe to enhanced notification as a service without the need of making large equipment expenditures.

iLinkx software products allow larger clients an opportunity to purchase the technology of enhanced notification outright, including all technical support and expertise needed to expand an existing system or the purchase and capital investment of a new one.

Applications

Residential

Commerical

Industrial

Milling/Mining

Manufacturing/Treatment

Chemical Plants

Institutional Facilities

Public Buildings

Military Sites

High Rises

Campus Complex's

Hotels/Conference Centers

Health Care

Airports

Marine

Clean Room Fabrication

Place of Worship

Train/Subway Stations

Amusement Parks

Resorts

Golf Courses

Fish Hatcheries

Agriculture

iLinkx receives industry proven "Contact ID" signals. For new and existing installations, this offers a substantial increase in the lifespan and usefulness of your equipment investment. Sites that have Digital Alarm Communicator Transmitters (DACT's) which report to monitoring services can easily enhance notification with a few minor programming modifications. Operating in an ancillary capacity, in accordance with National Fire Protection Association (NFPA) standards, iLinkx also receives alarm signals, independently processes the information and automatically dispatches without disruption to the current dispatch procedures of your existing monitoring service.

Interfacing is easy! There are no special hardware or expensive component requirements, nor are there any hidden cost or procedures. Simply go to our "Services" tab and subscribe to iLinkx service. Upon activation, you will receive iLinkx account information allowing you to enable your DACT/s alternate account feature (a rarely used option of existing UL Listed equipment) to also report information to iLinkx. You will then begin to unleash the power of your internet network placing critical information into the hands of first responders, management, and staff, including those agencies with a need to know.

Experience tomorrow's technology today with the automatic dispatch of text messages, emails and colorgraphic images. Avoid the high capital expenditure of additional computing stations, software, licensing and the associated labor of staffing such an operation. Enhance your notifications and reduce your response times, while minimizing the cost of operations, training and maintenance.

iLinkx receives industry proven "Contact ID" signals but for larger systems, iLinkx will receive all industry standard transmission protocols including wireless and (IP) internet based signals. For new and existing installations, this offers a substantial increase in the lifespan and usefulness of your equipment investment. Both existing and new sites can easily enhance notification with a few minor programming modifications in the field. iLinkx operates in an ancillary capacity, to any existing or new receiving equipment, in accordance with National Fire Protection Association (NFPA) standards. iLinkx independently processes the information and automatically dispatches without disruption to the current dispatch procedures of your existing receiving equipment or monitoring service.

Interfacing is easy! There are no special hardware or expensive component requirements, nor are there any hidden procedures. Simply go to our "Services" tab and request a proposal for iLinkx as a product. A team of experts will be assigned to promptly assist you and explain how you can

unleash the power of your internet network and place critical information into the hands of first responders, management, and staff, including those agencies with a need to know.

Experience tomorrow's technology today with enhanced notification and the automatic dispatch of text messages, emails and colorgraphic images in addition to the industry standard conventional receiving information. We provide complete NICET Level IV and/or Professional Engineered (PE) services. Whether you need assistance with project concepts, management, or safety coordination, our quality control team will help select the best products and services for your application needs.

Avoid the pitfalls and costly expense of proprietary specifications which only drive up cost and result in expensive sole source equipment procurements. Our professionals will introduce you to the concept of open architecture, open protocol, and non-proprietary equipment, using readily available, standard, off-the-shelf products. They specialize in helping select from the latest technology of headend receiving equipment, console racks, software, panels, and field devices. This allows for a more efficient and competitive approach to equipment design, engineering, purchase, installation, testing, training, certification and warranty. All services provided by our experienced and trained professionals. The service doesn't stop there though, they will assist in the ongoing maintenance and contract support services needed to protect your investment and maintain the highest level of service available to ensure you receive maximum performance during the entire lifecycle of your investment. Allow us to enhance your notification and to reduce response time when those critical seconds determine safety over disaster.

Text messages provide rapid notification, typically within 45 seconds from occurrence and display critical information for those needing to know.

Blackberry Devices expand the enhanced notification platform to include an emailed .pdf attachment in full color reflecting the exact location of the incident.

Personal Computers expand the enhanced notification platform even further, allowing greater viewing opportunities, printing and archiving information for future reference.

Agency Dispatch Centers get the information into the hands of first responders, during precious moments that distinguish safety from disaster.

Cellular Text

Frequently asked questions

Q: Can iLinkx text message my cell phone, and if so, how?

A: Cell phone text messaging, or "SMS" text messaging, is not the same as instant messaging on your computer. They're two very different systems. That doesn't mean all is lost, however. There

are some things that iLinkx can do very well. How much depends mostly on the cellular provider, and the type of phone you have.

SMS Text Messaging, SMS stands for Short Message Service, and is designed specifically for cell phones. iLinkx can usually send an SMS message to a cell phone via email. Most of the cell phone providers have a special email address or domain that you can send a message to, which then gets forwarded as a text message to the cell phone. For example with Verizon in the U.S., you can email #####@vtext.com, where "#####" is replaced with the 10 digit cellular number, and that message will get sent as a text message to that phone. Other carriers typically have some type of equivalent and/or a web page from which you can send a text message to one of their phones.

Important: remember that this is a Short message service ... usually only up to a certain number of characters of your message will be sent. Some providers will simply truncate your message if it's too long, others will break it up into multiple messages. Others might well discard the message. Check with the provider in question.

In addition, to the iLinkx received message, one can also forward the message via SMS on a phone to an email address. In all cases, remember that this is email based, and that response times may vary somewhat, depending on the carrier.

Blackberry Devices

Instant Messaging:

Q: Can iLinkx text message my Blackberry device, and if so, how?

A: Through IM services, like AOL's AIM, MSN's Instant Messenger and others, all are designed for what is called "computer to computer" services. They all assume that you have a computer of some sort. Many Blackberry devices these days pretty much are computers and run things like the Palm operating system, or a version of Windows that allows the receipt of emails and attachments in a somewhat limited or abbreviated form.

Because so many Blackberry devices have internet capability, it only stands to reason that iLinkx would find instant messaging and email notifications a useful tool for enhancing notification on Blackberry devices. In somecases, using an unlimited data access plan one is able to run the Mundu IM instant messaging client and chat using MSN Instant Messenger account, or an AOL Instant Messenger account. The only caveat here is that you must have an internet capable Blackberry device and have signed up for an internet data plan of some sort.

Q: Can iLinkx send an actual colorgraph image to my Blackberry device, and if so, how?

A: Yes. ilinkx automatically generates a colorgraphic image, immediately after receiving a signal, reflecting your floorplan, site location or whatever image you have provided us with. On

that image, a bold rectangle is placed around the specific device, sending the signal as well as a text description is automatically placed at the top edit line of the image. The image is then processed and transmitted to you as an easily opened .pdf attachment and sent to you via email in a matter of just a couple of seconds, not minutes, that the industry has found acceptable in the past.

Q: How large is a typical iLinkx .pdf attachment?

A: That obviously depends on the image and information being displayed however, it has been our experience that a 20,000 square foot floor plan with 50 devices located on it, will yield approximately a **250-300k** .pdf file in approximately 2 seconds. (This is approximately 2% - 3% of what a typical email mailbox will receive) The iLinkx process is what is key to this reduced file size and processing time. The benefits become enormous in internet transmission speed, computer screen build times, printing and overall computer management.

Personal Computers

Personal Computers continue to play a larger and larger role, not only in our lives but in the way we are conducting our communications. As technology has improved, monitor displays have also improved. This is where iLinkx really stands out in performance. The methods used by iLinkx in processing signal information, recording it, and automatically dispatching it, in a manageable form is what sets us apart.

The clarity of graphics are unsurpassed and non distorting, even when significantly zoomed in or magnified. This allows much larger colorgraphics images to be transmitted, in a much smaller packets, thus minimizing transmission time, computer screen build times yet provides easily opened attachments, using open protocol, non-proprietary, open architecture .pdf software.

In addition to viewing, messages and attachments are easily printed, in color, archived and even forwarded and made available to others automatically or manually, again using open protocol, non-proprietary, open architecture software, readily supporting mass notification and signalling systems.

Typically, the colorgraphic images are much better displayed on desktop monitors or even laptops because of the improved resolutions that the monitor displays now have. Using standard, open protocol reader programs such as Adobe or other .pdf based readers, one can easily arrange zooming, printing, saving, and even editing features for easy use.

Agency Dispatch Centers

The iLinkx Enhanced Notification Systems is ideal for new or existing Dispatch Centers. Using open market protocols, standard off the shelf hardware and proven application software modules, the iLinkx system operates in an ancilliary capacity to existing or new receiving equipment. The system is fully automated and processes all information independently and

automatically to produce the desired dispatch resulting from a signal or signals received, without any operator intervention whatsoever. The following is a description of how the integrated software modules operate.

iTranslate:

The itranslate software module is a continuously running program utilizing a windows based platform, operating in a minimized state to avoid impeding the background of any currently displayed windows. It is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version is fully integrated, in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the translation module automatically restarts and reloads into the resident operating system without any operator intervention.

iMonitor:

The iMonitor software module contains the setup information to control all activity logging. Additionally, it records a date and time stamp of all signals processed and the post-translated condition of the signal. The information is permanently recorded for historical data retrieval at a later date through the use of the iReport software module. The iMonitor software module determines and controls the overall number of authorized notification points of the Ancillary Notification System by the use of an internal software authorization key. The iMonitor software module is a continuously running program utilizing the windows platform and is minimized to avoid impeding the background of any currently displayed windows. It is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version is fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the iMonitor software module automatically restarts and reloads into the resident operating system without any operator intervention.

iWatch:

The iWatch software module contains all of the dynamic activation of text and graphic information to be dispatched to the designated recipient's device/s. The designated recipient devices may include, but not be limited to Blackberry's, Cell Phones, e-mail, Fax Machines, Laptop Computers, Desktop computers, Servers and Pagers.

Upon receipt of a signal, the iWatch software module begins an automatic processing sequence of the graphic information to be dispatched. The information is automatically and electronically generated in a Portable Document Format (.pdf) and stored for retrieval by authorized operators. iArchive software folders are automatically created for each facility account to archive the .pdf files by event and the date and time that they were received and processed. Each iArchive file is individually identified by the respective facility number and contains the exact date and time to the second of the activated event. The .pdf file is available to be access through common windows

programs for viewing and file maintenance requirements. It shall be possible for an authorized operator to view all devices by the simple click of the PC Mouse button contained on the Watch software display screen. Special maintenance alerts, historical data or any text information can be separately stored for each device, by authorized operator reference. The iWatch software module is a continuously running program utilizing the windows platform and is minimized to avoid impeding the background of any currently displayed windows. It is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version is fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the iWatch software module automatically restarts and reloads into the resident operating system without any operator intervention.

iDispatch:

The idispatch software module controls all outbound email and text messages to be dispatch to the designated recipient's device/s. The device/s may include but not be limited to Laptop Computers, Desktop Computers, Servers, or any internet email addresses, Cellular Telephones, or Blackberry device/s. The iDispatch software module continually monitors all outbound file messages and upon receipt, dispatches the designated information. The information is be dispatched in the form of text message/s, .wav file/s, graphical image/s, internet link, hyperlinks, and/or any pre-generated .pdf document/s. The iDispatch software module dispatchs all formats or any combination thereof in a single dispatch in a manner that allows cascade notification of unlimited recipients. Graphical images are dynamic in their operation allowing the recipient/s to zoom in or out of the image with no loss or degradation of the image/s. All signals are automatically dispatched, without any operator intervention in under, a total elapsed time of 75 seconds, from start to finish. The time shall be measured from when the actual field device (Smoke Detector, Pull Station, Water Flow, etc.) is activated to when a designated recipient receives the signal. All text message/s, .wav file/s, graphical image/s, internet links, hyperlinks, and/or any pre-generated .pdf document/s are device specific and not general in content. The specific location and all critical information shall be contained with each device dispatch. All graphic images are transmitted in .pdf format, and in color, reflecting the device in alarm in red, or device in trouble in yellow. All devices are reflected on the graphic image however only the abnormal device will be reflected in the designated color based on its condition. A quick locate feature (Bold Rectangle) shall be automatically generated and provided to draw additional attention to the abnormal device, even in a zoomed out condition. It shall be possible to zoom the image from 1% to 6,600% power or magnification. An Dispatch log file is automatically created each and every time a dispatch is made. The Dispatch log file is available to be accessed through common windows programs for viewing and file maintenance requirements. The iDispatch software module is a continuously running program utilizing the windows platform and is minimized to avoid impeding the background of any currently displayed windows. It is password protected and cannot be closed or shutdown by unauthorized personnel. A backup version is fully integrated in the event that a recovery operation from a catastrophic incident becomes

necessary. In the event of a complete windows operating system reboot, the iDispatch software module automatically restarts and reloads into the resident operating system without any operator intervention.

iConfigure:

The iConfigure software module is the utility program used for the inputting the configuration of all critical information into the Ancillary Notification System. Access to the program is by use of authorized passwords. Authorized personnel must sign on using a hierarchy of authorized password levels that have been established by the Master Administrator. Once signed on, authorized personnel shall have the ability to define each and every aspect of the signal and device characteristics. The iConfigure software module has an auto learn feature which enables field devices to be automatically imported into the iConfigure Software, avoiding manual entry of the devices and the associated device descriptor information, not with-standing, in the absence thereof, providing authorized personnel the ability to manually enter the device and descriptor information as an alternative. All Background images (Graphics) shall be programmed as sublevels of an image zone and an image group. All field devices shall be stored in a master database which shall be accessible easily from standard PC Mouse commands. Adding a device to an image consist of three simple mouse clicks to view the entire field device database followed by a simple drag and drop effort onto the respective image. When deleting or relocating a device, the device is simply removed from the image and automatically retained in the field device database for future placement. Editing a device allows authorized operators to change the specific device icon size or all of the device icon sizes contained on the image at one time without the necessity of leaving the edit command screen. After any given device or all of the field devices have been placed onto an image, it is possible to test the dynamic operation of any field device by selecting the device test option. This option allows verification of each field device alarm, supervisory, trouble and restoral functions in a virtual state or mode, as if it were an authentic change of event being received by the operating system.

iReport:

The iReport software module allows for a full history recap via a windows based, report query format structure, that can be entered by device address, type, condition, account, or date criterion and/or any combination thereof. All report results are displayed in less than 2 seconds, as a standard text file permitting easy printing in an open protocol, word merging, and/or text management arrangement. It is also possible to gather email and text message verification from the iArchive software module database for verification of email and text notification/s. A backup version of the Report log files are fully integrated, in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the iReport software module automatically restarts and reloads into the resident operating system without any operator intervention.

iArchive:

The iArchive module automatically stores a permanent record of the results of all system transactions to the system archive files. The iArchive software module resides as a separate and distinct database from the history report file and, to insure survivability, is not stored on the same computing device nor at the same computing location as the main operating system. It is possible to easily review the results of any and all transactions of the system at any time without the possible loss or interruption of the main operating system. The iArchive software module automatically restarts and reloads into the resident operating system without any operator intervention.

Mission Statement:

To enhance the notification of yesterday by developing technologies today that deliver the solutions for tomorrow; Through sincere dedication, unmatched quality and unparalleled service, iLinkx is committed to the success of each and every customer it serves. We understand that although our success is dependent on the innovation and level of service we provide, decisions are also based on value. Thank you to those who have chosen iLinkx among an ocean of options and alternatives.

Specifications:

iLinkx Receiving and Ancillary Notification Systems for Dispatch Centers, are also based on open market protocols using standard off the shelf hardware and proven application software programs which are comprised of two fully dynamic and integrated components. The following is a sample specification of those components:

The first component (Part 1) describes the Signal Receiving and Processing Equipment. This component allows operator intervention and defined procedures, which are executed by trained and qualified personnel to accomplish and produce the desired dispatch from the signal or signals received.

The second component (Part 2) is the dynamically integrated Ancillary Notification System which is fully automated and which processes its information independently and automatically, to produce the desired dispatch resulting from the signal or signals received, without any operator intervention whatsoever. Systems that do not demonstrate full dynamic integration, in compliance with the requirements of these specifications are considered substandard and unacceptable and will be rejected.

SIGNAL RECEIVING COMPONENT (PART 1)

LISTINGS AND APPROVALS

The system shall be listed by Underwriters Laboratory under Standards 864 (Control Units for Fire-Protective Signaling Systems), 365 (Police Station Connected Burglar-Alarm Units and Systems), 609 (Local Burglar Alarm Systems and Units), 827 (Central Station Alarm Services – AA High Line), 681 (burglar and Hold up Systems), 2050 (National Industrial Security Systems for Protection of Classified Materials), 1076 (Proprietary Burglary-Alarm Units and Systems), and 1610 (Central Station Burglar Alarm Units), . The system shall be UL Listed as a CENTRAL and REMOTE SUPERVISING STATION FIRE ALARM SYSTEM per NFPA 72 and as a PROPRIETARY SUPERVISING STATION FIRE ALARM SYSTEM when monitoring inputs other than DACTs. The UL Listing card shall show a (p) for proprietary Fire Alarm (Receiving Unit) under UL 864 category UOJZ.

Each processor controlled system module shall include an independent audible trouble signal (watchdog circuit) to indicate microprocessor malfunction. This is referred to as a "Supervised" configuration and is a requirement of the system operation.

Bidders shall provide UL documentation, accurate statements regarding all dimensions, detailed installation drawings, input power requirements, wiring requirements, and all other specifications required to make a complete evaluation of the system being proposed.

The system shall operate reliably in any environment comfortable to the human operator and shall have no special ventilation requirements.

Any variation from these specification requirements shall include a full explanation of all deviations or exceptions taken from the requirements contained within this document on a paragraph by paragraph basis. Bids or proposals that fail to address each paragraph and meet the minimum requirements specified herein shall be deemed non-responsive and will be rejected.

The Bidder shall be an authorized factory representative for the manufacturer of the equipment and all application software programs specified.

All equipment and application software shall be fully warranted against defects in both materials and workmanship for one year from the date of delivery.

The system shall be configured with the capability of monitoring 9 types of inputs simultaneously without the necessity of adding additional hardware.

1. (DACT) Digital Alarm Communicator Transmitters

The system shall receive alarms from Digital Communicators, Radio Transceivers and Internet Provided Interfaces. The following formats shall be accepted: (SESCOA, VERTEX, DCI, FRANKLIN FAST - 3X1), (SESCOA - 4X3), (RADIONICS HEX - 3X1, MODEM IIIa2 and BFSK), (Old ADEMCO, SILENT KNIGHT SLOW - 3X1), (ACRON - 4X1), (SILENT KNIGHT, NAPCO - 4X2), (CFSK, VFSK, SIA - MODEM), (FBI SUPERFAST, SUR-GARD, ADEMCO HI-SPEED, and (ADEMCO EXPRESS and ADEMCO CONTACT-ID - DTMF).

The system shall support up to sixteen (16) incoming receiving lines using combinations of dual port serial I/O modules and line card units.

A Line Card Unit shall contain a dual line Digital Alarm Communicator Receiver phone line card. The phone line(s), line card, and communications to the Line Card Unit shall be fully supervised and provide audible and printed indications of failure. Power on, off-hook and line loss conditions shall also be indicated by LED activity on the Line Card Unit front panel. The software shall support a 128-event buffer for unacknowledged events and up to six (6) hexadecimal digits of account number, four (4) hexadecimal digits of zone number, and 64 three-character event codes per account.

The system shall provide sufficient memory to allow the storage of field programmable English text descriptions for all accounts, their associated event codes, and input zones. The system shall allow up to 40 lines of 32 characters each for every account message, up to 4 lines of 32 characters each for every zone message, and a 16-character descriptor for each event code. Field programmable event code tags shall be available to allow prioritizing of DACT alarm events to insure the most appropriate and expedient response. Optionally, a "GROUP TROUBLE ACKNOWLEDGE" function shall be available. This function shall allow the acknowledging of signals, programmed with the trouble event code tag, as a group when activated by a single operator action from the "touch screen".

The system shall allow 24-hour test codes to be programmed for all compatible formats. The system shall have the ability to accept 24-hour call-in for transmitter verification, and annunciate a FAIL-TO-TEST alarm if the call-in is not received. The call-in time window shall be user selectable from 1 to 168 hours. The system shall receive Opening and Closing signals without operator intervention.

The system software shall allow dialer accounts to be put IN and OUT-OF-SERVICE. If an account is OUT-OF-SERVICE, all incoming transmissions from that account will be ignored. When a dialer account is returned to IN-SERVICE from an OUT-OF-SERVICE condition, all zones will be considered restored to normal at the receiver.

The system software shall support a Dialer Account TEST mode. If a Dialer Account is placed in TEST mode, all incoming signals will be printed in the standard alarm printout format and optionally stored in History. However, there will be no display or audible alert to the operator.

The system shall allow up to 500 dialer alarms to be included in the rotating, sequential, alarm display.

INTERFACING:

The system software/hardware shall be available without the Line Card Unit to support interfacing with third party digital receivers.

2. The system shall be capable of receiving serially transmitted alarm signals directly or via modems over dedicated phone lines from remote alarm monitoring systems, digital receivers, or Fire Alarm Control Panels. The communication link shall be supervised and, upon failure, the system shall annunciate a communications failure condition. These alarm signals shall be annunciated in a way that is specific to the type of alarm input received. These alarm signals shall be reported on a prioritized basis per UL 864.

3. The system shall be capable of interfacing to radio systems including the RADSCAN AlarmNet 7810 long range radio receiver, the LARSNET RCI3300 and RCI4000, and the Keltron RF7300 – AES Intellinet receiver, via RS-232c. All received alarms shall be annunciated in a way that is consistent with alarms received from DACTs. All field programmable, fixed field, English text annunciation capabilities and outputs shall be supported. It shall be transparent to the operator whether these events were received via Radio, IP or DACT.

4. The System shall also accept all direct connect and multiplex inputs and support all hardware and software outputs of the receiving System. The inputs accommodated shall include reverse polarity, end-of-line resistor, dry contacts, proprietary tones signals, private line or star multiplex and distributed multiplex as well as coded (McCullough) Fire Alarm signals.

SYSTEM OPERATION:

When a change in any of the In-Service inputs occurs, the system shall sound the audible alert, display the appropriate message, and print the appropriate message. In order to silence the audible, the operator must touch the ACK control. Touching this shall cause the audible to silence, and the ACKnowledge message to be printed. This message shall remain displayed until CLEAR is touched, whereupon, the system returns to its regular standby operation. If the operator does not touch ACK, the audible shall continue to sound, but no further printing shall occur for that event.

Inputs that are not in the secure condition shall become part of a display sequence. In case of multiple events are on the list each event shall be displayed for 5.0 seconds in chronological order. Once the end of the list of abnormal points is reached the list shall scroll automatically to the beginning of the list and start displaying the list of events start again. Touching FAST SCAN shall speed this to once every 1.0 seconds. In addition to non-Secure zones, the sequential or rotating display will include a screen for accounts out-of-service and a screen for accounts in test mode.

SIGNAL OUTPUTS:

Relay Outputs - The system shall have the capability of controlling up to 96 normally open or normally closed Form-A relay contacts. The relays shall be mounted 16 to a plug-in circuit board and be accessible from the rear panel. Relay operation is to be completely programmable via the plug-in keyboard, with provisions for up to four (4) relays being energized by one input.

The relays shall have a rating of 400mA at 100VDC, 10VA max. The output connections are to be made by means of a 25 pair standard telephone connector for ease of installation. Relay outputs shall be field programmable by event code for each individual account and will be cleared upon operator acknowledgement.

Transistor Outputs - The system shall have the capability of controlling 288 open collector transistors (OCTs). The OCTs shall be mounted 48 to a plug-in circuit board, and be accessible from the central system processor. OCT operation is to be completely programmable via the plug-in keyboard, with provisions for up to four (4) OCT' to be energized by one input. The OCTs shall be able to sink 100ma at 48VDC. The output connections shall be made by means of a 25 pair standard telephone connector for ease of installation. Transistor outputs shall be field programmable by event code for each individual account and will be cleared upon operator acknowledgement.

Auto/Manual Transmitter Output - The system shall have the ability to either automatically or manually transmit a coded signal. There shall be two output relays, and each relay shall be set to any one of sixteen (16) speeds from .25 sec to 4 seconds. The relays shall be rated at 220VDC, 215mA, at 60W max. These coded output relays can be individually set by an internal switch to operate in either Type "A" or Type "B" Mode, with Type "B" mode being defined for Positive Non-Interfering Successive service. The transmission shall be accomplished by either accessing the touch screen for manual output, or by preprogramming individual zone and condition codes via the keyboard for automatic output. Default operational parameters, e.g. speed and number of rounds, shall be set by on-board dip switches which can be overridden by preprogrammed operational parameters for automatic operation. The transmitter shall be a plug-in circuit board that is accessed from the central system processor. Special ALL-OUT and MULTI-ALARM Software applications that transmit specially prefixed coded signals shall be optionally available.

RS232C Output - RS232C ports shall be available which can transmit data upon receipt of an alarm in three modes. Mode 1 will send the 4 lines of the message printed on the internal Dot Matrix Printer. Mode 2 will output the first 10-line display screen from the edited data base message. Modes 1 & 2 shall be printed in 32 or 64 character lines. Mode 3 will output the RS232C data using Radionics protocol to interface to a computer, another monitoring system or a central station automation software package.

Manual Relay Control - As an option, the system shall allow the manual control of relay and transistor outputs by the operator from the Touch Screen. The outputs shall be energized, de-energized, or momentarily energized.

PRINTER:

The printer shall have a minimum of 32 columns to allow instructions to be presented in an efficient manner. The instructions should provide a permanent record of an event, including the time and date of an event for recall purposes.

The printer shall allow the dispatcher to have printed messages or sets of instructions, which shall be field programmable. The messages or instructions can be removed from the printer to take to the site of the event for reference purposes.

Upon alarm receipt the system will print four fixed lines. The first two lines include an alarm or restoral indication, the account number, a time and date stamp, the alarm receiver number, event code description if programmed, or event code default, and the zone number. The last two lines printed shall be field programmable. They shall be the first line of the account message and the first line of the zone message. The alarm printout shall be printed in red or black for special emphasis. The acknowledge printout is always black and is the same as the first two lines of the alarm printout, except it indicates acknowledge instead of alarm and prints the time and date of acknowledgement.

For ready availability and low cost, the printer shall be able to use commercially available plain 3" roll paper.

If desired, fanfold paper should be usable to allow collection in a fanfold catch tray.

To assure the permanence of the record, the printout must not fade with time, as is the case with thermally sensitive paper.

DISPLAY:

The display shall have "touch screen" operating controls to provide the operator with detailed menu-driven instructions for each operator function and maintenance-free operation.

The display is used to present messages or instructions when an event occurs. The display shall be a cathode ray tube (CRT) at least seven (7) inches in size to allow major details of messages to be presented in a single display.

Character size shall allow the operator to read the display from a distance of ten feet. The CRT shall have an orange or green phosphor screen for lower operator fatigue, and direct etch for glare-free viewing. Video attributes shall be used by the system to segregate the fixed format message display screens. Dialer alarms shall be displayed using a fixed format rather than free format messages as are used for other alarm input types. The event information is displayed in separate fields or areas on the display screen. Some fields shall be mandatory. Other fields shall be optional as programmed by the user.

Mandatory fields include the Account Number, Zone Number, programmable event code, and time and date of event. Un-programmed event codes shall be displayed as received with the word 'CODE'. Programmed event codes will display their 16-character description on the alarm display screen. For SIA and Contact-Id formats, the system will automatically annunciate the event code description.

The system shall allow a total of 296 lines of 32 characters each to be programmed for the account and zone descriptions. The alarm display screen shall allow a total of seven (7) programmed 32 character lines to be displayed. These seven (7) lines shall be a combination of account and zone description message lines. All zone message lines shall display on the alarm and acknowledge screens. The system shall allow a maximum of four (4) zone message lines to be programmed for each zone. This leaves three (3) lines that will be displayed in the account message display window on the alarm screen. At least two (2) lines will be reserved for zone messages, even if blank. The maximum size of the account message window shall be at least five (5) lines. Additional programmed account message lines will be accessible only from the acknowledge display screen. The remainder of the account message shall be scrolled through the account message display window by using the NEXT page and BACK page touch switches.

Unprogrammed account or zone description fields shall be blank. There will be a single alarm display screen for any given dialer event composed of the fixed fields, programmable fields, and the touch screen area.

CLOCK/CALENDAR:

The clock portion shall provide military time (24 hour) in hours, minutes and seconds. The calendar shall provide month, day and year. Once set, the calendar shall run automatically with no need to be reset at any time including leap years. A printout shall be made each time the clock/calendar is changed to record that a change was made.

The clock/calendar shall run on 60Hz as available from the power line with its attendant accuracy, averaging less than one second per month deviation. When placed on battery operation, the unit shall automatically switch to a crystal-controlled time base, internally generated, averaging +/- 13 sec/month.

As an option, the system must be capable of synchronizing the real time clock to the National Institute of Standards and Technology (NIST) atomic time standard, via a Synchronized Master Clock from Spectracom or Chronolog Corporation or an approved equal.

MESSAGE CAPABILITY AND EDITING.

Messages can be of various sizes. If an average message size is 256 characters, a minimum capacity of 1000 messages shall be provided with the system with expansion to 20,000 messages possible. Each message shall use the message storage area in multiple blocks of 128 characters each, according to its size, to allow for efficient use of memory space. The system shall support a minimum of 3 megabytes of internal memory.

The system memory shall not have to be removed from the system to be erased or programmed. An installer level password shall be required to access system diagnostics which support hardware and memory testing.

Editing shall be accomplished via a full computer-style keyboard. The keyboard can be disconnected without disturbing normal alarm monitoring. Incoming alarms shall interrupt the edit process. After alarm acknowledgement and dispatch, a single control shall be provided to resume the edit process at the point of interruption.

CONTROLS:

All controls used in the normal operation of the system shall be long life and non-mechanical.

The controls shall be presented on the face of the CRT. Intersecting that area of the CRT screen displayed as a control, either by touching or by placing a finger or similar object just in front of the screen, shall cause activation of that control. This type of control shall allow multiple uses of the controls area with up to 16 different controls displayed simultaneously. Some indication of control activation shall be provided; either an obvious system action will take place or audible feedback shall be provided.

When no changes are being processed, the operator shall be presented with the following controls.

FEED:

This shall cause the printer paper to advance.

STOP:

This shall cause the display to freeze on the current screen.

FAST:

Inputs in an abnormal state shall be displayed sequentially on the CRT screen with a 5 second period. Touching FAST shall cause this period to be 1 second.

NEXT:

Touching this control button shall cause the screen to change and display the following control buttons.

DIALER-ACTIVITY:

This control shall cause the screen to display a Keypad, allowing the operator to select any programmed dialer account alarm input to the system. All dialer activity status changes shall be accomplished with this control. This includes placing accounts Out-of-Service, In-Service and in Test mode.

DISPLAY MESSAGE:

This control shall cause the screen to display a Keypad, allowing the operator to select any alarm input to the system, and to display its programmed display message.

SET CLOCK:

This appears only if the key switch is enabled. This control shall cause the screen to display a Keypad, allowing the operator to set the date and time.

PRINT MESSAGE:

This control shall cause the screen to display a Keypad, allowing the operator to select any alarm input to the system, and printout its programmed print message.

PRINT:

This shall cause "PRINTER OK" plus "TIME & DATE" - to be printed.

LIST:

This control shall cause the printer to list the account numbers and the total number of accounts both Out-of-Service and in Test mode.

CLEAR:

This control shall cause the display to return to normal display sequencing.

RETURNING TO THE NORMAL DISPLAY SEQUENCE:

STOP:

This shall stop the sequential display to allow examination of a particular message. Also, this shall cause the touch area beneath the displayed message to change to include:

CLEAR: This returns the display to its normal sequencing routine.

FEED: This control shall cause the printer paper to advance.

When a change of state occurs, the audible alert sounds and the appropriate messages shall be printed and displayed. Also, this shall cause the touch area beneath the displayed message to change to include:

ACK: Touching this shall cause the Acknowledge message to be printed and displayed and the audible to be silenced. This screen shall also display the FEED control button. After ACK is activated, the screen shall change and display the CLEAR and FEED control buttons.

SOFTWARE OPTIONS:

HISTORY - A battery backed internal RAM storage facility in which to automatically record all operations performed by the Receiver shall be provided. Accessibility is menu driven from the keyboard. A minimum of 4080 events shall be provided per single storage facility. Expansion to 16,352 events shall be possible by adding additional memory capacity and a software upgrade. An external computer shall not be required. Actions recorded shall include Alarm Activations, Restorals and Acknowledgements, In/Out Service functions, Clock Set functions, Master Clock failures, Edit sessions, AC loss alarms, Communication failures, and all System Supervisory alarms. The history record shall be printed or displayed in its entirety, or sorted by account, time, type, priority, and date or in any combination thereof.

The system shall be connected to a PC either locally or via modems. A password will be required to permit system access. This connection shall be for the purpose of database backup, restoral, creation, editing, archiving, printing, or remote programming. This connection shall be transparent to the operator and must not affect alarm receiving in any way.

EDITOR PASSWORD - The system shall be capable of providing password protected database access. This shall limit access to the programmed message database to authorized personnel.

BACKGROUND ALARM PROCESSING - The system shall provide the ability to permit alarms from a remotely monitored location to be passed through an operating system on the way to their final destination without operator interruption. If the signal transmission path is interrupted, the last system before the point of interruption becomes the dispatch location.

CALL ASSURANCE CHECK-IN - Optional software shall be available for institutions such as Assisted Living Facilities. The purpose of the "Call-Assurance Check-in" software is to reduce staffing requirements, by automating the supervision of these people who shall be self-reliant, but require daily confirmation of their physical and mental well-being due to their age, physical condition or mental health. With this system, the residents shall be required to manually activate a signal to the receiver. Reception of proper check-in signals on enabled accounts is normally transparent to system operators. The receiving system's receipt of the correct signal validates the monitored persons "up and about" status. The absence of this signal within a predetermined time period will be treated as an alarm. An exception report, containing those accounts that have not yet checked in, is printed automatically upon expiration of the predefined time period. This alarm event printout signifies the need to physically check on those persons who have not yet reported in that they shall be "up and about".

FT-OPTION - The system shall be capable of dedicating any or all operator's consoles to receive a particular alarm type. The Central System Processor, when equipped with a video display, will annunciate all alarm types. The fire alarms shall go to a particular operator's console at the Fire Department, and the Burglary or Hold-Up alarms shall go to a separate operator's console at the Police Department. In the unlikely event of a system failure all alarms will be annunciated on the operational operators console without regard for the FT-Option.

OPERATOR LOG-ON/OFF - The system shall be capable of providing operator accountability by requiring the operator to LOG-ON with a unique password before alarm acknowledgements will be accepted. LOG-ON/OFF activities shall be recorded in the optional system history file.

NETWORKED SYSTEMS - The system shall be capable of supporting the connection of multiple system processors with alarm receiving and dispatch capabilities. Also supported shall be redundant databases with automatic updates between locations and cross-acknowledge functions.

PHYSICAL DETAILS - The Dialup phone line inputs shall be connected to the line card that is cable connected to the central system processor unit. A standard telephone connection shall be used at the system.

The panel operator's unit shall be inclusive to all operators' functions. The panel operator's unit shall run on 24VDC, filtered, regulated power. The power supply shall be mounted remotely from the panel operator's unit, and shall be powered by 115VAC, 60Hz, and provide terminals to float-charge a pair(s) of 12V solid cell batteries. The batteries shall be supervised and an output provided at the power supply for a no/low battery condition. If AC input power fails, the panel operator's unit shall run on batteries without interruption, and an audible alert shall sound indicating battery operation. Any system AC power failure shall cause a supervisory alarm at all panel operators' units as well as at the central processor, if equipped for annunciation.

All phone line inputs will be connected to the central system processor. The central system processor shall be available with no display, a video display, or video display and printer. A maximum of four remote operator's consoles can be provided per system. The operator's console(s) and central system processor will communicate via RS422 for distances to 4000 feet, and via modems for further distances. Operator's consoles will be available with video display only, or video display and hard copy printer. Communications between the processor and the operator's consoles shall be supervised and provide visual and audible indications of failure. System programming shall be accomplished from any operator's console or the system processor with the display option.

Auxiliary Functions:

When the paper supply becomes low, the screen shall so indicate by displaying PAPER LOW in the lower right hand quadrant. In addition, the audible alert shall be sounded briefly once per minute. The FEED button becomes an "E" control, which when activated permits access to printer feed and print commands. When the paper supply is exhausted, PAPER OUT shall be indicated, and the alert will be sounded as for PAPER LOW. In this case, no further hard copy record will be available until paper is replenished. Events to be printed will be stored and then printed when the paper is replaced.

Should the printer become jammed, the words HEAD JAM will be indicated, and the alert will be sounded once per minute.

OPTIONAL HARDWARE:

Any system module with a CRT Display screen shall be capable of driving an external video monitor via a 75ohm coaxial cable to provide a redundant display only, no controls.

The system shall be capable of interfacing to external line printers via RS-232c, RS-422, or modems. Operating modes one or two shall be selected as well as 32 or 64 character lines. This option shall be added to the operators' consoles or the central processor.

The system shall be capable of transmitting alarm event data to alphanumeric pocket pagers via either an on-site system or off-site commercial paging system provider.

The system shall be capable of interfacing to Central Station Automation Software, PC GRAPHICS, and Computer Aided Dispatch Systems.

The system shall be capable of supporting redundant system processors. The system shall provide a seamless, automatic, switch over function with no loss of account and zone status or database information in the event of primary processor failure.

Life Safety Event Management Software:

The system shall provide detailed information and specifications for a single and multi-user life safety event management automation, graphical display, and dispatch system including all required hardware and software. The software enhances the functionality and utility of the alarm receiving systems or third party alarm receiving and monitoring systems.

The life safety event management system integrates proven reliable alarm monitoring systems with state-of-the-art computing technologies to dramatically increase the capabilities of life safety organizations. The system shall provide a highly efficient access to information that shall enable fast and accurate response to life safety situations.

A reliable and versatile Windows-based system combines the most valuable features of central station automation and graphical display software for fire alarm panels, with proven alarm receiving technology to produce a system that meets the mission critical needs of today's life safety industry.

System Architecture - Performance:

The system is designed to provide high performance and quick dispatch. The dispatch functions shall be separated from database maintenance and monitoring functions to minimize the impact of administrative requirements on the dispatcher while providing a high degree of security and reporting information to the systems administrator and managing stakeholders.

The modular design of the system architecture makes it robust, scalable and extensible. Modular design shall enable specialized software components to perform specific functions efficiently, quickly and accurately without interference from unrelated components. The architecture is built on a standard operating system, using known interfaces and connection methods, with extensive network and printer support.

The central core of the software architecture is the Event Manager module. The primary function of the Event Manager is to maintain the list of active events and alarms and control access from competing client modules. It shall provide continuous backup shadowing to preserve the latest state of all active events in the unlikely event of system interruption.

The Event Manager module acts as a server for various client modules that can originate, manipulate, or display events. Because it has no database connections and very little dependency on system resources, it is very robust, very efficient and very small. Even when under a load of several thousand alarms, it consumes a small fraction of system resources.

To ensure reliability, and minimize the dependency of any specific function on system resources, individual client applications perform different functions, independent of one another.

Examples include:

1. Receiver clients provide the interface to external alarm receiver hardware systems. They manage the unique requirements of the communications link and protocol, isolating these details from the rest of the system, and provide complete event information to the event manager. New receiver clients can be developed with no impact on the Event Manager or any other client module.
2. Supervisory Clients perform specific background tasks such as monitoring periodic device check-in, logging alarms, and monitoring disabled devices and recording events to history.
3. User Interface Clients, like the dispatcher, shall be designed to be intuitive for the user.
4. Interconnection Clients connect multiple redundant system functionality.

The clients shall communicate with the Event Manager through a single, well-defined interface. This interface shall provide the same functional connection whether the Event Manager and the clients reside and run on the same machine or on two machines separated by thousands of miles.

System Features:

The system shall UL Listed to receive alarms from a wide variety of standard industry technologies including Ethernet, active network and long-range radio, star and distributed multiplex style inputs, digital dialers, direct connects (POTS or fiber), and coded signals. It can also accept alarm inputs directly from industry-standard alarm receivers. The system shall enable

fast and efficient communication to the server by providing a customized, ODBC-compliant database that facilitates efficient, accurate alarm dispatching and tracking. Color-coded alarms and custom audio/visual indicators enable instant recognition of the nature and/or severity of an event. Full graphic capabilities shall enable the user to import graphic files to enhance the dispatcher's speed and accuracy and blinking icons that quickly identify the devices in alarm.

The system shall include an integral history reporting function for analyzing historical trends and tracking false alarms. Powerful and flexible search capabilities enable systems administrators to locate and segregate information by entering one or more key words. The standard, open systems database shall enable the administrator to employ third-party reporting tools to provide custom reports when necessary.

The system Server, shall be a dedicated, rack-mount or tower, high-performance server, forms the core of single- or multi-user systems. Stand-alone or rack-mount PC workstations use a standard Windows-based operating system and components to provide sufficient resources for all installed applications.

The system shall provide an advanced Intel Pentium processor, an 8.4-inch diagonal TFT color display with an optional easy-to-use touch screen or familiar keyboard-and-mouse operation, and an optional quiet thermal printer with automatic take-up.

Mounted in a standard 19-inch rack, the workstation is configured to fit a wide variety of dispatch consoles. External video and printer outputs shall be available to easily incorporate industry-standard printers and large-screen displays. The LAN interface shall enable operator workstations to be networked together with the server.

The expanded networking capabilities enable multiple users to access the system simultaneously with varying levels of privileges to perform many tasks such as maintaining customer account information, reviewing event history and active, on-line alarm dispatching. Internet accessibility is also available for feature additions or remote diagnostics.

Functionality:

The system shall provide unique features that meet the wide variety of requirements inherent in the life safety market. The system engineers and product managers shall maintain an extensive schedule of software enhancements shall be generated through ongoing customer and market research.

Supervisory Functions:

The supervisory function monitors a variety of types of alarm and system activity including periodic device check-in, out-of-service and test service mode settings, receiver interface communications link integrity, and system status, such as logging, ticket or report printer availability and status.

When the system detects a problem in these areas, the problem is reported to the operators as a supervisory alarm, and includes a detailed description of the out-of-normal condition.

In addition, the Supervisory Client station shall provide event logging and history recording services.

Rotational display screen:

The system shall provide a view of all active events by continuously displaying these events at five second intervals. This ensures that unresolved issues shall not be lost or forgotten.

Unlimited accounts:

The number of alarms accepted by the system is restricted only by the limits of the computer hardware.

Automatic signal prioritization:

The life safety event management software shall automatically prioritize all alarm signals according to UL standards using programmable event classes.

System response modes:

The system shall support programmable response modes including:

1. User - for full system control
2. Auto-log - to alleviate operator interaction
3. Ignore - for automatic discard of received events

Operational and disable modes:

The system operator shall set the service mode of any connected panel or device to active, out-of-service or test mode.

In active mode the system will annunciate all events from the panel and its devices, according to the default or programmed colors, sounds and display tab preferences. In out-of-service mode, events shall be tracked and recorded by the system but not reported to the operator. When a panel or device is returned to active mode from out-of-service mode, its last recorded status will be reported to the operator if the device is not restored to normal. When a panel or device is returned to active mode from test mode its last recorded status will not be reported to the operator. Disable modes will have a selectable duration and will automatically lapse or shall be manually cancelled by the operator

Group acknowledge:

The 'group acknowledge' function shall enable the operator to batch acknowledge a group of low priority events such as trouble and restore events, so that higher priority events can be managed expeditiously.

Swinger Suppression:

A 'swinger' is an alarm input that constantly toggles between normal and off-normal states presenting hundreds of identical events to the system for processing and operator interaction. The system shall provide a swinger suppression function that prevents the operator from being overloaded with such a huge number of alarms that effective response is impossible. It prevents exhaustion of system resources, even if the system is left unattended for very long periods of time, by reducing the number of spooled printer jobs, and reducing the size of the backup shadow file.

This feature prevents operator frustration and overload by reducing the workload to manageable levels. Thousands of swinger events shall have occurred, but the operator need only respond to the two initial alarms. Swinger suppression prevents the system and operator overload problems by accumulating repeating events together in a single compact form.

When the first trouble event comes in and generates an event on the screen, the system shall sound the audible alert, displays the pending alarm banner, and prints an event record. When the second signal from that alarm is received, if it's the same event code from the same device, no new alarm is generated. If it's a different event from the same device, a new alarm will be generated, printed, logged and, if it is a higher priority (e.g., a fire vs. a trouble) it will take over the pending display.

If the device keeps going back and forth between the trouble and alarm condition, no new pending alarms shall be generated, thus the operator only responds to the pending fire and trouble events.

The history tab shows several pieces of data on that event:

1. The first occurrence of the event
2. The most recent occurrence of the event
3. The number of times the event reoccurred
4. A detailed audit history of the event

After one swinger alarm has been acknowledged, the process starts all over again: the next occurrence of an event will generate a new alarm in the system, but further occurrences will, as above, accumulate into that pending alarm.

Storm mode:

Setting the system to 'storm mode' allows certain events, such as those caused by severe weather, to either be auto-acknowledged or ignored for the period of time the system is in this mode. Non-restoral events shall be maintained in rotation until cleared by restoral signals or manual deletion. At the end of this time, the system automatically reverts to normal operations.

The systems administrator can define which classes of events will be affected along with the automatic expiration period for storm mode.

Sounds:

Audible (.wav) files shall be imported into the database and linked to incoming alarms for automatic operator notification.

Printing:

The system shall use any Windows-supported local or networked printer for the following functions:

Logging - logs every incoming alarm and its acknowledgement with a brief, multi-line entry. The system shall employ line-oriented, impact or thermal printers for this application.

Ticket printing - prints a single page of information about a specific event. A site shall use either line printers or page printers. Ticket printing is a summary of the dispatch information available on different tabs on the screen. It includes the 'banner', i.e., the alarm type, consolidated location summary and time of occurrence, location, personal contact/key holder information, instructions, site location and info, subscriber and locale name.

Report printing - supports printing the hardcopy output from History Editor, Monitor or third-party applications such as Crystal Reports. Either line or page printers can be used, though laser page printers produce higher quality output in shorter time.

Default operation for un-programmed events:

The software shall provide full support for an intelligent, operator-friendly display of events arriving from un-programmed sources. The software supports intelligent message interpretation of a variety of industry-standard message types, including Ademco - Contact ID format, direct-connect, distributed multiplexer formats, radio formats and SIA-compliant formats, and understands more than a thousand different messages and variants.

When the system is installed, it not necessary to perform extensive programming in order for the system to be immediately usable for operators. When the system receives a message from any of a variety of industry-standard signaling devices, an intelligent interpretation and display of that

event is displayed for the operator. Only the physical location of the monitored system must be programmed.

To facilitate quick event response, instead of presenting obscure event codes, the system clearly displays the nature of the events in prioritized hierarchy. Further programming shall add important functional capability, such as site- and device-specific instructions, customized graphics and audible alerts.

Multi-user features - Remote access:

The system shall provide remote access through standard networking protocols over high-speed TCP/IP links. Remote workstations provide the same level of functionality as the host seat, limited only by the system access privileges that shall be determined on an operator-by-operator basis. Open networks employ a recommended hardware router for secure network communications.

Remote stations can be used not only for regular dispatch access, but for system administration and configuration, as well as history maintenance, auditing and reporting.

Security - Operator Privileges:

To increase security and ensure compliance with published policies and procedures, the system shall provide multiple levels of privileges for operators, users, guests and administrators. For example, operators shall acknowledge and resolve events but not clear them from the system, or a user must have a given level of privilege to access the history tool.

Dispatching:

The system shall provide a main dispatch screen displays all the critical information a dispatcher requires to expedite event management. The system immediately displays the most critical and basic information, with extended support information only a single click away. Basic dispatch information includes the nature of, location, time and date of the event. Extended information includes complete site description and location information, detailed dispatch instructions for the monitored site, call and contact lists, graphic display information including maps and floor plans showing the exact location and the nature of the alarm, photographs and diagrams, account information, and details that shall be used in diagnosing faulty or run-away devices and managing defend-in-place or hazmat situations.

When an alarm is acknowledged, a programmable dispatch tab appears. Normally, the dispatch tab is displayed showing instructions, location and contact information. This setting does not limit access to the other tabs - the operator shall access any tab by clicking it.

Rotation events shall be programmed to appear by class. Rotation retains the last state of the device. Normally, the system retains all off-normal states including both Alarms and Troubles. Restores to Normal, under these conditions, clears an off-normal event from rotation.

Dispatch Operation:

The operator log-in function shall provide an audit trail to track and analyze the alarm monitoring and dispatch function.

The system shall provide an acknowledge screen upon receipt of an event. This first screen displays the nature and location of the event with a programmable color background and a programmable audio component to alert the operator to the type of event. The second screen that is displayed after operator acknowledgement is the dispatch screen. This screen shall provide detailed information on the type of event, location of the event, and the recommended response steps and procedure. The system shall be programmed to display prioritized contact information. The dispatch screen shall provide user access using either a keyboard/mouse or touch screen-activated tabs to the other types of informational screens available to the operator.

1. The 'dispatch' tab returns the operator to the initial dispatch screen.
2. The 'maps' tab shall provide access to graphical depictions of the location and type of event.
3. The 'site' tab shall provide access to information identifying the actual physical location of the monitored system or building and any critical information pertaining to that location such as hazardous materials and any other data specific to that site.
4. The 'notes' tab shall provide the operator with the ability to maintain a running real time record of all action taken and reported in response to the received event.
5. The 'details' tab shall provide the operator or technician with the technical information pertaining to the type of alarm, receiving technology and pertinent notes for that alarm.
6. The 'history' tab shall provide the operator access to the history of that specific event including the event ID, raw event data, time of receipt, time dispatched, source, operator, how many times it was received, and time resolved.

The universally familiar Windows tool bar at the top of the screen shall provide access to the file, service mode and search, event, tools and help pull down menus.

1. The file menu shall provide access to login and logout functions.
2. The service mode menu shall provide access to panel and device control for disabling and enabling alarms.

3. The search menu allows database search by all fields.
4. The tools menu shall enable manual alarm entry and storm mode activation.
5. The help menu shall provide full on-line user documentation.

The operator shall click on the 'alarms pending' window at any time to see list of all events that have been received and shall be pending operator acknowledgement. The operator will see the event priority and shall select an event from the list for acknowledgement, dispatch and resolution. All resolved events shall be accompanied in history by an operator selected resolution code. This code aids in historical trend analysis.

Programming:

Use of the configuration database maintenance application requires the user to log in with a recognized password and privilege level. Logon privileges, as set by the system administrator, determine the level of access to the systems database.

Existing sites or accounts shall be updated or added using the configuration database maintenance application.

The system shall provide the ability to add extended site information such as contacts (key holders, supervisors, and other related personnel), site-specific instructions, detailed explanatory notes, and warnings. In addition, the user shall import and associate graphic images such as maps and floor plans that illustrate this information and can help the dispatcher to quickly and accurately respond to an event.

The system supports programmed receivers, locales, device templates and event categories. Some of this data is pre-configured from the factory. Other data is programmed during the initial setup.

The receiver object is supported by receiver interface software clients. The receiver object shall provide a programmable tab displays such as general, configuration, and locales.

The locale can be associated with a physical entity or several physical entities as well as with a single receiver or multiple receivers.

The user shall be able to add information about the hardware devices that are monitoring that site.

All access to and control of the database maintenance application is provided through two methods: the navigator, which shall provide a graphic-oriented hierarchical view of the database, and the menus. While many functions can be accessed either way, there shall be some that shall be only available through one method.

For those functions accessible by both, the choice is a matter of convenience or preference. Accessing elements of the database is general and not constrained by how the various elements and layers relate to one another. For example, it is easy to use the search menu to find any device in the system, whereas it shall be simpler to find a device belonging to a particular site using the navigator.

The navigator window is divided into two 'panes'. The left pane shows a hierarchical directory of the database. The right pane displays the detailed contents of each layer selected from the hierarchical directory.

The left pane of the navigator is the Navigator Directory, displaying each level in the database hierarchy. Required for programming a device is an icon and a label for Receivers, Locales, Subscribers, Sites, and Devices, as well as entries for Service Companies, Event Categories, Contacts, Authorities, Operator Groups, Operators and Device Templates. Click any of these and the right window displays the contents of that level.

The Navigator Directory shall provide quick-access functions including; add, search, expand and collapse.

The database maintenance application shall provide a comprehensive menu of functions to provide access control, set display mode, search for items or add new ones, and configure different aspects of the system.

The menus include: file menu, view menu, search menu, new menu, and tools menu.

1. The file menu shall provide the exit function.
2. The view menu shall enable the programmer to choose from iconic, list or detailed viewing of the right navigator pane objects.
3. The search menu shall enable the operator to search for any editable database object.
4. The new menu shall enable the programmer to add an object to the database.
5. The tools menu shall provide dispatch options, printer, storm mode and group dispatch setup.

To add a new site or account to the database, the user should have the following information readily available:

1. General information for the site or account such as the name/description, the account number (if any), physical address and site telephone number.
2. In which Locale the site is located.

3. The type and identification number, account number or hardware address of the hardware that is used to monitor the site; for example, the particular model of radio transceiver or the connection point for a direct-wire device.

4. Optional contact information such as key holder name and phone numbers, graphics information such as maps or floor plans, subscriber information and if the site is one location of several under a single subscriber.

The maintenance application shall enable the user to pre-program general support information before adding information for specific signaling devices. Examples include objects such as:

1. Service companies
2. Operator groups and individual operators
3. Event categories
4. Device templates

Each of the major entities in the database (Locales, Subscribers and Sites) shall provide the option of programming a designated service company - the organization responsible for installing, maintaining and upgrading the equipment and systems.

1. The Locale object supports authorities, service companies, notes, sites and contacts programming.
2. The Site object shall enable general, device, contact, graphic, instruction and note tab programming.
3. The General tab allows the programming of information such as address, with locale, service company and subscriber fields being selectable from a list and filling the appropriate field automatically. The site name and ID shall also be programmed on the General site tab.
4. While the Site represents the monitored area, the devices provide the association between physical messages from a remote sensor and the high-level information about the site.
5. The Contacts tab shall enable the programming of call lists and selection of a primary person.
6. The Graphics tab shall enable the user to associate graphics such as maps, floor plans or images with the site. The number of graphics that shall be associated with a device is unlimited.
7. The Instructions tab shall enable the user to enter site-specific instructions to be displayed to the operator when an event occurs at the site.

8. The Service Company entry supports programming entry tabs of clients, contacts, and notes.
9. The system allows devices to be added and shall provide general, zones, event codes, icons, and instructions tabs.
10. Zone information shall come from a template or be programmed individually for each device.
11. The Event Codes tab shall provide the connections or mappings between the device's low-level hardware event codes and the pre-programmed event categories.
12. The Icons tab shall enable the user to place icons on the graphical images.
13. The Event Categories entry generates operator-friendly, comprehensive actions in the database.
14. The Instructions tab shall enable the administrator to enter detailed instructions that shall be specific to the device being programmed. The instructions will be displayed along with the event category instructions when the device signals an event.

The system shall allow the user to program direct connect devices as zones. The supported programming tabs shall be general, event codes, icons, and instructions. The General tab supports device ID, template selection, site, receiver, location, and zone. The system shall enable the user to program the subscriber object. The supported programming tabs shall be: general, sites, contacts and notes.

The system shall provide multiple levels of access privileges through the use of operator groups. Each operator group can be assigned different levels of privileges. Individual operators can be added to operator groups, and shall be given the privileges of that group. The system supports multiple operator groups, each with its own privilege mask combinations.

The system supports the programming of default behavior in response to received events including sounds and colors.

The system shall provide device template architecture. This shall enable the user to program a complex panel or device model only once. Adding new customer accounts using device templates is very fast, efficient and reliable. These features substantially reduce programming time and programming errors all of which minimize setup costs. The user can easily change global device behavior, such as check-in-times, on multiple devices by changing the device template, reducing ongoing maintenance time and expense. Template behavior shall be overridden partially or totally for account- or zone-specific behavior through account and zone programming, without invalidating existing templates.

Database:

The system includes an ODBC database that shall enable ANSI-compliant SQL access.

Schemas shall be public and published.

An XML importer is functional, to allow the user to import other databases.

The system supplier shall provide online utilities for database maintenance such as backup/restore, version upgrades, and like functions.

Graphic Files:

The system shall support multiple graphic file formats. Files shall be attached to an incoming alarm and linked in a hierarchy so navigation, can be performed by the operator. This shall enable the system to receive an alarm and automatically display a street map and/or subsequent graphics of the building, wing, floor, room, and finally to the device icon.

The following file types shall be directly imported into the system:

1. .BMP, .RLE - Windows bitmap graphics files
2. .GIF - Graphics Interchange Format files
3. .JPG, .JPEG - Joint Picture Experts Group format files
4. .PDF - Portable Document Format
5. .WMF, .EMF - Windows graphics metafiles
6. CAD files must be 100% transparent and compatible with these file formats.

The system application software shall support multiple hierarchical graphic images creating important instruction and/or images:

In an emergency situation, multiple hierarchical graphics shall provide the dispatchers with the most accurate and efficient method of understanding the physical situation of an event. This approach to graphical file presentation shall be full dynamic and not put any additional burden on the operator to manage a graphics environment while in the midst of managing with mission-critical events.

The system's graphic structure shall enable the administrator to provide a mix of images: beyond the normal maps and floor plans, the administrator can include photographs of attending personnel or of specific areas, providing the facility optimal flexibility and versatility. Using dedicated images also minimizes system resource requirements.

Monitor application:

The Executive Monitoring utility shall provide the site administrator or supervisor with a way to monitor basic system activity and status from any appropriately-configured local or remote workstation computer. This function shall be available only for monitoring the system status and shall provide no means to directly modify events.

The monitor utility shall provide a display of the following important system activities and states:

1. Active events: all currently active events shall be displayed. Separate windows provide displays of all new, pending, in dispatch, on hold, resolved and in rotation events. Any event can be selected to display the details associated with the event, including extensive site-specific information.
2. Disable devices and zones: Any device which is placed in out-of-service, test or other disable modes is displayed, along with site information and expiration time.
3. Operators: a window displays all logged on operators by operator name, system name and log-in time.

History:

The system shall provide full history recording capability. History data is stored to an ODBC-compliant database separate from the main configuration database to minimize impact on the main database resources. This allows the databases to reside on physically separate volumes.

The history system records the following important system events:

1. All real-time events, such as alarms, troubles and restoral's originating from real devices through event receivers.
2. Operator-generated manual alarms.
3. System-generated supervisory events such as missed check-ins, receiver communications failures, printer faults, etc.
4. Device service mode changes.
5. Operator logins and logouts.

Where appropriate, a complete history for each event state change, such as acknowledgement, resolution and eventual removal is captured, including details of when the transition occurred, and the operator responsible.

History editor:

The system shall include an online history editor and viewer application that shall enable the user to instantly view the contents of the system's history database. Functional features shall include:

1. Search on different criteria, such as locale, subscriber or site name/number, event type, current event status, and dates
2. Sort event display on any displayed attribute
3. View event details of any selected event
4. Add short notations to events (requires appropriate operator privileges)
5. Add updated or final resolution of events (requires appropriate operator privileges)
6. Print a report of selected and sorted events on any networked Windows-based printer. Operator shall choose to print all or just selected events.
7. Erase selected events from history database (requires appropriate operator privileges)

System configurations:

The system shall be available in a range of configurations to meet the individual needs of different facilities. These configurations shall be combined in a variety of ways to allow system configurations for alarm monitoring applications ranging from single-package, single user stand-alone or rack systems to full receiving rack-based servers supporting multiple operators over secure LAN and WAN connections.

Systems that are installed on an open network shall be configured to include routers/VPNs at each access point, so as to protect the system from unauthorized access.

System hardware and operational specifications

Standard hardware includes:

- 4U standard rack-mount chassis with integral, dual, hot swap, 400 watt 120/240 VAC power supplies
- ATX form-factor motherboard
- Dual Quad Core Processors
- 8GB of memory, expandable to 32 GB
- SVGA or better display system
- 10/100 LAN Ethernet port

- 10 USB 2.0 ports
- Wireless keyboard and mouse interface
- One parallel port (rear)
- Multiple serial ports
- Internal 3 TB high-capacity disk storage
- 2 - Integral 52X CD-RW drive
- Built-in 8.4" high bright LCD (300 nits)
- Rack-mount keyboard/mouse shelf
- Redundant high-performance, high-reliability SCSI-III multiple-drive RAID configuration with real-time background data shadowing.

ANCILLARY NOTIFICATION COMPONENT (PART 2)

The system software module shall, upon receipt of a signal, translate the format in which the signal was received to determine the designated facility name/ number, the specific address of the device sending the signal, the designated type of device, and the condition or state of the device. (Alarm, Supervisory, Trouble, or Restore) Once the information is received it will be automatically processed to the Monitor software module of the Ancillary Notification System. The translation software module shall be fully programmable to translate all signals from any manufacturer's panel in an open protocol without the possibility of loss of information or interruption of service.

iTranslate:

The itranslate software module shall be a continuously running program utilizing the windows platform and shall be minimized to avoid impeding the background of all currently displayed windows. It shall be password protected and shall not be closed or shutdown by unauthorized personnel. A backup version shall be fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the translation module shall automatically restart and reload into the resident operating system without any operator intervention.

iMonitor:

The iMonitor software module shall contain the setup information and control all activity logging. Additionally, it shall immediately record a date and time stamp of the signal being received and the post-translated condition of the signal. The information shall be permanently recorded for historical data retrieval at a later date through the use of the Report software

module. The Monitor software module shall determine and control the overall number of authorized notification points of the Ancillary Notification System by the use of a software authorization access key issued by the manufacturer. The Monitor software module shall be a continuously running program utilizing the windows platform and shall be minimized to avoid impeding the background of all currently displayed windows. It shall be password protected and cannot be closed or shutdown by unauthorized personnel. A backup version shall be fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the Monitor module shall automatically restart and reload into the resident operating system without any operator intervention.

iWatch:

The iWatch software module shall contain all of the dynamic text and graphic information to be dispatched to the designated recipient's device/s. The designated recipient devices shall include, but not be limited to Blackberry's, cell phones, e-mail, fax machines Laptop computers, Desktop computers, Servers and pagers.

Upon receipt of a signal, the Watch software module shall begin an automatic processing sequence of the graphic information to be dispatched. The information shall be automatically and electronically printed in a Portable Document Format (.pdf) and stored for retrieval by other authorized operators. Archive software folders shall be automatically created to store the .pdf files by event and the date and time that they were received and processed. Each Archive file shall be individually identified by the respective facility number and shall contain the exact date and time to the second of the event. The .pdf file shall be available to be access through common windows programs for viewing and file maintenance requirements. It shall be possible for an authorized operator to view all devices by the simple click of the PC Mouse button contained on the Watch software display screen. Special maintenance alerts, historical data or any text information shall be separately stored for each device, by authorized operator reference. The Watch software module shall be a continuously running program utilizing the windows platform and shall be minimized to avoid impeding the background of all currently displayed windows. It shall be password protected and cannot be closed or shutdown by unauthorized personnel. A backup version shall be fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the Watch module shall automatically restart and reload into the resident operating system without any operator intervention.

iDispatch:

The idispatch module shall control all outbound email and text messages to be dispatch to the designated recipient's device/s. The device/s shall include but not be limited to Laptop computers, Desktop computers, Servers, or any internet email addresses, cellular telephones, or

Blackberry device. The Dispatch module shall continually monitor all outbound files and upon receipt, dispatch the designated information. The information shall be dispatched in the form of text message/s, .wav file/s, graphical image/s, internet links, hyperlinks, and/or any pre-generated .pdf document/s. The Dispatch module shall dispatch all formats or any combination thereof in a single dispatch to unlimited recipients. Graphical images shall be dynamic in their operation allowing the recipient/s to zoom in or out of the image with no loss or degradation of the image/s. All signals shall be automatically dispatched, without any operator intervention in under, a total elapsed time of 75 seconds, from start to finish. The time shall be measured from when the actual field device (Smoke Detector, Pull Station, Water Flow, etc.) is activated to when a designated recipient receives the signal. All text message/s, .wav file/s, graphical image/s, internet links, hyperlinks, and/or any pre-generated .pdf document/s shall be device specific and will not be general in content. The specific location and all critical information shall be contained with each device dispatch. The graphic images shall be transmitted in .pdf format, shall be in color, reflecting the device in alarm in red, or device in trouble in yellow. All devices shall be reflected on the graphic image however only the abnormal device will be reflected in it designated color based on its condition. A quick locate feature (Bold Rectangle) shall be automatically generated and provided to draw additional attention to the abnormal device, even in a zoomed out condition. It shall be possible to zoom the image from 1% to 6,600% power or magnification. An Dispatch log file shall be automatically created each and every time a dispatch is made. The Dispatch log file shall be available to be access through common windows programs for viewing and file maintenance requirements. The Dispatch module shall be a continuously running program utilizing the windows platform and shall be minimized to avoid impeding the background of all currently displayed windows. It shall be password protected and cannot be closed or shutdown by unauthorized personnel. A backup version shall be fully integrated in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the Dispatch module shall automatically restart and reload into the resident operating system without any operator intervention.

iConfigure:

The iConfigure software module shall be the utility program used for the inputting the configuration of all critical information into the Ancillary Notification System. Access to the program shall be by use of authorized passwords. Authorized personnel must sign on using a hierarchy of authorized password levels that have been established by the Master Administrator. Once signed on, authorized personnel shall have the ability to define each and every aspect of the signal and device characteristics. The Configure software module shall have an auto learn feature which enables field devices to be automatically imported into the Configure Software, avoiding manual entry of the devices and the associated device descriptor information, not with-standing, in the absence thereof, providing authorized personnel the ability to manually enter the device and descriptor information. All Background images (Graphics) shall be programmed as sublevels

of an image zone and an image group. All field devices shall be stored in a master database which shall be accessible easily from standard PC Mouse commands. Adding a device to an image shall consist of three simple mouse clicks to view the entire field device database followed by a simple drag and drop effort onto the respective image. When deleting a device, the deleted device shall be removed from the image but shall be retained in the field device database for future replacement. Editing a device shall allow authorized operators to change the specific device icon size or all of the device icon sizes contained on the image at one time without the necessity of leaving the edit command screen. After any individual or all of the field devices have been placed on an image, it shall be possible to test the dynamic operation of any field device by selecting the device test option. This option shall allow verification of each field device alarm, supervisory, trouble and restoral functions as if it were an authentic change of event being received by the operating system.

iReport:

The iReport software module shall allow a full history recap via a windows based report query format structure that can be entered by device address, type, condition, account, or date criterion and/or any combination thereof. All report results shall be displayed in less than 2 seconds, as a standard text file permitting easy printing in an open protocol, word merging, and/or text management arrangement. It shall also be possible to gather email and text message verification from the Archive software module database for verification of email and text notification/s. A backup version of the Report log files shall be fully integrated, in the event that a recovery operation from a catastrophic incident becomes necessary. In the event of a complete windows operating system reboot, the Report software module shall automatically restart and reload into the resident operating system without any operator intervention.

iArchive:

The iArchive module shall automatically and permanently record the results of all system transactions to the system archive files. The Archive software module shall reside as a separate and distinct database from the history report file and, to insure survivability, shall not be stored on the same computing device nor at the same computing location as the main operating system. It shall be possible to easily review the results of any and all transactions of the system at any time without the possible loss or interruption of the main operating system. The Archive software module shall automatically restart and reload into the resident operating system without any operator intervention.

Scalability:

The life safety event management system shall be designed using open protocol and standard off the shelf technology with the capacity to surpass all current and projected future requirements by at least 500%. The system shall provide software application modules that use open protocol and off the shelf proven technology and shall be specifically designed for multi-building and

municipal facility life safety environments to ensure a minimum 15 year system life of high-performance and reliable service. The system shall provide all required functionality with new or existing alarm monitoring and receiving equipment to monitor, receive, interpret, annunciate, respond, track, dispatch, electronically notify, and manage all life safety events.

System Software:

The software shall be an extensible application using the Microsoft Windows operating system platform. The software shall be provided on a standard platform enabling the system to be integrated with other facility, municipal and campus management systems such as mass notification, paging, CAD, CCTV and video display and IP accessible systems.

Support Documentation:

Provide the following support documentation:

- A network setup guide that establishes the requirements and procedures for site administrators to use when
 - incorporating the system into a network.
- A server installation guide that shows the installation and configuration of the Server.
- History editor and user guide.
- Operators manual including Graphic Compositions.
- A database programming and maintenance manual.
- A quick dispatcher's guide to show basic operator interaction with the system providing the ability to acknowledge
 - events and dispatch personnel.
- A full dispatchers' training course presented in Microsoft PowerPoint format.
- Online, fully indexed and searchable user documentation.