



UniNet™ 2000 Specification
Integrated Facilities Management Monitoring and Control Systems
Version 2.1
04/12/2002

UniNet 2000™ is a trademark of Notifier©

INDEX

Alarm Monitoring	8	Incident Reporting Module.	11
APPLICABLE PUBLICATIONS.....	4	INSTALLATION:	13
APPROVALS	4	INSTRUCTION/TRAINING	14
CCTV.....	9	NIONs	5
Computer Network	6	Photo Imaging Client	11
CONTROL ASPECTS OF SYSTEM		Reports & Logs.....	9
SOFTWARE	9	Routers/Repeaters/Bridges	6
FACILITY MANAGEMENT FUNCTION		Security and Card Access	9
CAPABILITIES	8	SUBMITTALS	3
FINAL INSPECTION.....	14	SYSTEM EXPANSION	9
GUARANTY	14	SYSTEM SETUP & CONFIGURATION	14
Guard Tour Client.....	12	UNINET™ NETWORK.....	5
HARDWARE	4	Wide Area Adapter	6
History Manager	8	WORKSTATION SOFTWARE	7

THE FOLLOWING NEEDS TO BE INCLUDED IN THE FIRE ALARM SPECIFICATION:

HARDWARE SECTION:

Fire alarm panel shall provide printer port for industry standard printer protocol. The printer shall communicate with the control using an interface complying with Electrical Industries Association standard EIA-232D.

Fire alarm panel shall provide standard RS 232 CRT port for ASCII terminal operation.

SUBMITTALS SECTION:

Where the proposed fire alarm system does not have a UL 864 listed interface by the Facilities Monitoring System manufacturer (a list of UL 864 Listed systems shall be provided by the Facilities Monitoring System manufacturer upon request) the following shall be provided:

Provide the protocol for the RS 232 printer port and CRT terminal ports of the fire alarm panel including pin assignment and timing charts.

Provide CRT terminal emulation requirements and protocol including escape sequences for basic fire panel system operation including Acknowledge, Signal Silence and System Reset.

Provide typewritten list in columnar format of each alarm, trouble, off-normal condition, restoration to normal of any point or system status, operator acknowledged events, and any off-normal & restore event transmitted through the CRT and printer ports of the fire alarm panel.

Submittals that do not include the required fire alarm printer/CRT port information shall not be accepted.



1. INTEGRATED FACILITIES MONITORING SYSTEM

This section of the specification includes the furnishing, installation, and connection of a PC based graphical facilities monitoring system including Underwriters Laboratories (UL) listed application software and hardware complete and ready for operation. It shall include, but not be limited to, one or more PC based graphical workstations, all input/output devices, network communications media, control equipment, auxiliary control devices, power supplies and wiring including fiber optic media as shown on the drawings and specified herein.

- 1.1. The system shall utilize an advanced technology network to monitor and control fire, security, card access, and CCTV and other facility information over a LonWorks network. The system shall allow a mixture of different technologies and manufacturers' equipment to operate on the same network and provide the operator with a consistent look and operation for all monitored equipment. The system shall support a variety of

topologies and media and shall provide an industry standard open architecture transport layer protocol.

- 1.2. The scope of this section of the specification is to provide a single system consisting of one or more workstations for monitoring of multiple manufacturers monitoring systems in multiple buildings.
 - 1.3. Using standard RS 232 ports on existing and future monitoring and control systems used by the facility, the system shall connect to and interpret status change data transmitted from the ports and provide graphic annunciation, control, history logging and reporting as specified herein. Proprietary network systems that cannot interface to existing addressable fire alarm systems at the facility or systems requiring the use of a "dry contact" or "voltage monitoring" interface shall not be accepted.
 - 1.4. The basic system shall be Underwriters Laboratories (UL) listed to Standard 864 (fire), 294 (Card Access) and 1076 (Security).
 - 1.5. The system shall comply with requirements of NFPA Standard No. 72 for Proprietary Signaling System Receiving Unit except as modified and supplemented by this specification. The system shall be electrically supervised and monitor the integrity of all conductors.
 - 1.6. The system and associated equipment as specified herein shall be manufactured 100% by a single U.S. manufacturer (or division thereof). The manufacturer shall be of the highest caliber and quality. An ISO 9001 certified company shall manufacture the system.
2. SUBMITTALS
- 2.1. General
 - 2.1.1. Ten copies of all submittals shall be submitted to the architect, engineer, and owner for review.
 - 2.1.2. All references to manufacturer's model numbers and other pertinent information herein are intended to establish minimum standards of performance, function and quality. Equivalent equipment (compatible UL listed) from other manufacturers may be considered as a substitution for the specified equipment as long as the minimum standards are met.
 - 2.1.3. Substitute equipment proposed as equal to the equipment specified herein shall meet or exceed the minimum specified standard. For equipment other than that specified, the contractor shall supply proof that such substitute equipment equals or exceeds the features, functions, performance, and quality of the specified equipment.
 - 2.2. Shop Drawings
 - 2.2.1. Sufficient information, clearly presented, shall be included to determine compliance with drawings and specifications.
 - 2.2.2. Wiring diagrams shall indicate all wiring for each item of equipment and the interconnections between the items of equipment.
 - 2.2.3. Include manufacturer's name(s), model numbers, ratings, power requirements, equipment layout, device arrangement, complete wiring point-to-point diagrams, and conduit layouts.
 - 2.3. Manuals
 - 2.3.1. Submit simultaneously with the shop drawings & submittals; complete operating manuals and technical data sheets.
 - 2.3.2. Provide a clear and concise description of operation that gives, in detail, the information required to properly operate the equipment and system.
 - 2.3.3. Approvals shall be based on complete submissions of manuals together with shop drawings.

- 2.4. UL 864, 294, 1076
 - 2.4.1. Provide a list of monitoring systems by model number including Fire Alarm, Security, CCTV, and Access Control systems currently UL listed to standard to operate with the proposed Facilities Monitoring System.
3. Certifications
 - 3.1. Together with the shop drawing submittal, submit a certification from the major equipment manufacturer indicating that the proposed supervisor of installation and the proposed performer of contract maintenance is an authorized representative of the major equipment manufacturer and factory trained on all equipment contained in the submittal. Include names and addresses in the certification.
 - 3.2. Provide NICET Certification documentation for factory authorized field technicians performing field final connections and system programming.
4. APPLICABLE PUBLICATIONS:
 - 4.1. The publications listed below form a part of this specification. The publications are referenced in text by the basic designation only.
 - 4.2. National Fire Protection Association (NFPA) – USA.
 - 4.3. No. 70 – National Electric Code (NEC).
 - 4.4. No. 72-1996 – National Fire Alarm Code.
 - 4.5. Underwriters Laboratories Inc. (UL) – USA.
 - 4.5.1. No. 50 – Cabinets and Boxes.
 - 4.5.2. No. 864 – Control Units for Fire Protective Signaling Systems.
 - 4.5.3. No. 1076 – Proprietary Burglar Alarm Units and Systems.
 - 4.5.4. No. 294 – Access Control System Units.
 - 4.5.5. No. 1481 – Power Supplies for Fire Protective Signaling Systems.
 - 4.6. Local and State Building Codes.
 - 4.6.1. All requirements of the Authority Having Jurisdiction (AHJ).
5. APPROVALS:
 - 5.1. The system shall have the following UL listings:
 - 5.1.1. UL Standard 864 (fire).
 - 5.1.2. UL Standard 1076 (security).
 - 5.1.3. UL Standard 294 (access control).
6. HARDWARE:
 - 6.1. The product(s) shall be manufactured by as provided by NOTIFIER®. Model numbers specified are those of NOTIFIER® and are to establish the minimum standard of operating characteristics and quality. Substitute equipment proposed as equal to the equipment specified herein shall meet or exceed the minimum specified standard. For equipment other than that specified, the contractor shall supply proof that such substitute equipment equals or exceeds the features, functions, performance, and quality of the specified equipment.
 - 6.2. All equipment and components shall be new, and the manufacturer's current model. The materials, equipment and devices shall be tested and listed by a nationally recognized approval agency.
 - 6.3. Computer:
 - 6.3.1. The system shall be a UniNet™2000 Facilities Monitoring System. The UniNet 2000 system shall operate on an IBM compatible UL listed Intel Pentium III processor operating at no less than 800 MHz. The workstation shall have: no less than 256 megabytes of RAM, a hard drive with no less than 20 Gigabytes of storage space, a minimum of 8 megabytes of video RAM, a CD-R/W for system backup, internal supervisory CPU watchdog board with audible annunciator, 100 Base-T Ethernet NIC card, and a mouse type pointing device.

- 6.3.2. The UniNet™ NETWORK computer shall come equipped with all necessary gateway modules to allow connection to the network it monitors as standard equipment. All workstations shall support Ethernet communications when multiple workstations are required.
- 6.3.3. A UL listed Ethernet Hub shall be provided for connection of multiple workstations, servers, clients, event managers, and/or network printers.
- 6.3.4. The UniNet™ NETWORK computer shall support an SVGA monitor and be supplied with a 19" monitor.
- 6.3.5. The computer shall be capable of networking to additional computers and these computers shall be capable of operating as workstations and/or Local Area Servers or Wide Area Servers. Alarm annunciation shall appear on all workstations and may be silenced at each local workstation. However, only one workstation and operator shall be in command of system alarm acknowledgement at any time.
- 6.3.6. A hot standby local area server option shall be available to manage the Echelon network.
- 6.4. Printer:
 - 6.4.1. Support one or more Hewlett-Packard HP Laser Jet, or equal, printers to be located and connected each workstation for graphics and report printing.
 - 6.4.2. Support one model PRN-5, 80-column dot matrix tractor feed industrial grade printer for event and date-stamped printouts of off-normal events and status changes per workstation.
7. UNINET™NETWORK:
 - 7.1. The UniNet™ network shall consist of a Free Topology network utilizing twisted pair copper media in a bus, star, T-tap, or ring style 7 configuration at 78 Kilo baud. Transmit/receive twin fiber strand FT-10 point-to-point topology shall also be available.
 - 7.2. Network interface software shall be by the same manufacturer as the hardware portion of this specification.
 - 7.2.1. The UniNet™ network shall provide the option to support network segments operating at 1250 kilo baud over an Echelon FO-10 network utilizing single fiber strand multi-mode bi-directional fiber media in a bus or loop configuration.
 - 7.2.1. The UniNet™ network shall utilize Network Input / Output Nodes (NIONs) to interface between the individual buildings' systems to be monitored by the UniNet™ network. The NIONs shall act as a translator from the building system's specific panel communications protocol to the UniNet™ network protocol as well as serve as a transceiver from the building system panel to the UniNet™ network.
 - 7.3. NIONs shall be available in configurations that will allow transparent communications via RS 232 serial data ports with intelligent fire alarm control panels, security systems, CCTV systems and card access systems.
 - 7.3.1. NIONs shall be available in configurations that will allow monitoring of dry contacts, switched voltages, conventional security devices, access control panels and conventional fire alarm control panels utilizing scheduled, automated and manual control.
 - 7.3.2. NIONs shall be UL listed to Standard 864, 294 and 1076 and be provided with their own enclosure or be available in rack mount configurations.
 - 7.3.3. NIONs shall be available in configurations that will allow monitoring and control of access control devices and capable of operating stand-alone or as a member of the network. Such NIONs shall be UL listed to Standard 294.
 - 7.3.4. NIONs shall operate at 24 VDC and obtain their power from the monitored control panel or a UL listed battery backed auxiliary power supply. All terminals shall be transient protected to 2400V and LEDs shall be provided for status, service and diagnostics.

8. Computer Network:

8.1. The UniNet™ network shall be capable of monitoring a minimum of 100 nodes (NIONS and routers) on a local area server consisting of, but not limited to, intelligent or conventional fire alarm control panels or a competitor's intelligent or conventional fire alarm control panels. In addition, up to 99 local and wide area servers shall be connected via Ethernet for a total local area combination of up to 12672 (99x128) total local area nodes. Wide area servers shall also be available for remote building operation via a Building Communications Interface (BCI). Each BCI shall control up to 32 remote NIONS at each remote building. A single WAN server equipped with up to 10 UL listed TPI-BCI modems shall control up to 75 remote BCI's.

8.1.1. Computers shall be networked using Ethernet supporting the use of TCP/IP protocol for local area systems.

8.1.2. The UniNet™ computer network shall also support fault tolerant Class A Ethernet operation. A break in the network media shall be annunciated. The network shall also have the capability of annunciating the location of a single break, provided the network topology information has been entered.

8.1.3. This network shall be capable of supporting multiple clients (i.e. workstations, configuration applications, automated response applications, etc.) and up to ninety-nine (99) servers.

8.2. Routers/Repeaters/Bridges:

8.2.1. The UniNet 2000™ network shall be capable of operation at a length of 4,000 feet using FT-10 topology without the need for routers or repeaters when operating on approved wire. Routers or repeaters shall be required for distances beyond 4,000 feet. Utilizing FO-10 topology, the network shall be capable of operating at a length of 8,000 feet (10db of attenuation) between nodes (NIONS). In any event the complete monitoring system shall support at least 99 hardware servers Local area and or wide area servers shall be supported. Provide routers, repeaters or bridges where required to increase distance, alter network configuration or change media or to extend to remote facilities over alternate communications media including UL listed dial-up PSTN telephone, leased line, or non-UL listed single mode or multimode fiber or Ethernet connectivity. Dial-up units shall dial a local number and stay connected. Upon loss of carrier, a supervisory alarm shall be indicated at the workstation and the units shall automatically redial to connect.

9. Wide Area Adapter:

9.1. The UniNet 2000™ network shall utilize a Building Communication Interface (BCI) to monitor and control network segments as described in sections 6.2 and 6.3, over a wide area. These segments are free standing networks, supervised by the BCI.

9.2. Each BCI shall be capable of supporting up to 32 nodes (NIONS as described in section 7) per site.

9.3. Each BCI shall communicate with one or multiple workstations through one or multiple wide area servers utilizing dial-up PSTN for UL applications or X.25 connections for non-UL applications.

9.4. Wide area servers and workstations shall be capable of supporting multiple BCI sites.

10. WORKSTATION SOFTWARE:

10.1. System software shall be by the same manufacturer as the hardware portion of this specification.

10.2. The UniNet™ network will interface and report the individually monitored system's status via a user-friendly Graphical User Interface (GUI) based software workstation.

- 10.3. The GUI based software will provide a graphical representation of each facility being monitored with floor plans and icons representing the actual locations of the various systems; and / or sensors' locations.
- 10.4. The UniNet™2000 workstation shall provide voice annunciation of UniNet™ activities and a Voice Messaging option shall be included.
- 10.5. The UniNet™2000 workstation shall have the ability to support graphic printing of all UniNet™2000 data including graphical floor plans, system activity, history and guidance text. An HP 4020 LaserJet printer shall be supported for the graphics and report printer options.
- 10.6. The workstation software shall permit auto-navigation to the screen containing the icon representing the system or sensor in the event of an off-normal condition occurring. The icon shall indicate the type of off-normal condition (i.e. ALARM or TROUBLE) and shall flash and change to the color associated with the off-normal condition using RED for ALARM and YELLOW for TROUBLE.
- 10.7. The software will allow the attachment of text (.txt) files, sound (.wav) files, image (.bmp) files and video (.avi) files to each system or sensor icon allowing additional information to be provided to the system operator for responding to the off-normal condition. The system shall be capable of supporting multiple language sound files. Only one language at a time shall be utilized on each workstation. The software shall provide a library of device icons, information labels such as HAZMAT symbols, sound files (.wav) for speech annunciation of system conditions (Voice Messaging option).
- 10.8. The software shall allow the importation of externally developed floor plans in Windows Metafile (.WMF), or Bitmap (.BMP) format.
- 10.9. The software shall operate under Microsoft Windows 2000 as manufactured by Microsoft Corporation.
- 10.10. The software shall utilize a 1024 X 768 GUI display capable of showing a large primary floor plan display, a key map representative of a larger view of the primary display and its relationship to the facility being monitored, the current operator, number of fire, supervisory, pre-alarms, troubles, and security events including Card Access events within the UniNet™ network as well as outstanding events and acknowledged events.
- 10.11. The software shall provide auto-navigation to the screen containing the icon of any system or sensor when an event is initially annunciated. In addition, operator navigation to screens containing outstanding events shall be accomplished by "clicking on" the event from either the acknowledged or unacknowledged event.
- 10.12. The software shall contain a History Manager, which shall record all system events with a time and date stamp as well as the current system operator's name. The History Manager shall provide the system operator with the ability to record actions and comments associated with an off-normal condition of any system activity. The History Manager shall signal a need to back-up the history file at 100,000 events and then remind the operator at intervals of 100 events thereafter. It shall be possible to pre-select data fields for reporting and then saving the report as a template with a file name. It shall also be possible to schedule the pre-defined report to print at a designated time.
- 10.13. The software shall be password protected and provide for the definition of security profiles for operator access control.
- 10.14. The software shall have a capacity of at least 1,000 screens / floor plans or as dictated by hard drive space and installed VIDEO and RAM memory for efficient operation.
- 10.15. The software shall contain provision for defining monitoring profiles of pre-selected NIONs (Network IN/OUT NODES) for monitoring. I.e. the system administrator shall be

provided means to select which signals can be monitored by selected operator. This shall include provision for alarm types within the selected NODES.

- 10.16. The software shall contain provision for defining control profiles of pre-selected NIONS (Network IN/OUT NODES) for control. I.e., the system administrator shall be provided means to select which signals can be controlled by selected operator.

11. FACILITY MANAGEMENT FUNCTION CAPABILITIES:

11.1. History Manager:

11.1.1. The system shall provide for the ability to store all off-normal events experienced by the various sub-systems that are monitored by the system. All events shall be recorded with a time and date stamp and the system operator shall be provided with the ability to log a pre-defined response or a custom comment for each off-normal event and have that comment stored in the history file with the time, date and operator name.

11.1.2. The History Manager shall provide for the ability to conduct searches and generate subsequent reports, based on all events for a single system / device address, a specific node, a specific type of off-normal condition and date range (mm/dd/yy to mm/dd/yy) or combinations of these search parameters. The number of entries in the history file that match the determined search criteria will be displayed.

11.2. Alarm Monitoring:

11.2.1. The system shall provide for continuous monitoring of all off-normal conditions regardless of the current activity displayed on the screen. An example would be that if an operator is viewing the history of a sub-system and an off-normal condition should occur, the system shall automatically navigate to the graphic screen showing the area where the off-normal event is occurring.

11.2.2. The system shall prioritize all off-normal events as defined by Underwriter's Laboratories into the following categories: fire alarms, troubles, supervisory alarms, pre-alarms and security alarms.

11.2.3. The system shall display a running count of all events by type in an alarm event counter window. The event counter window shall include five counters, defaulted to Alarm, Trouble, Security, Supervisory, and Access Control Events. The user shall have the capability of reconfiguring the name of each counter and the type of events counted.

11.2.4. The system shall show a running list of all unacknowledged events and acknowledged events and allow the system operator to acknowledge an event by "double-clicking" on that event in the Unacknowledged Events box. The Unacknowledged and Acknowledged Events boxes shall contain an abbreviated description of the off-normal condition. The details of the condition may be viewed by "double clicking" on the Expand button located at the head of the unacknowledged events box.

11.2.5. The system shall allow the attachment of user-definable text files, image files and sound files, to each device / system monitored in order to facilitate the operators and response personnel's response to the off-normal condition.

11.2.6. The system shall record all events to the system's hard drive. A minimum of 100,000 events may be stored. The system shall issue a history file back up advisory after 100,000 events and a reminder after every 100 events thereafter.

11.2.7. Device addressing shall include 3 digit Node Address, 3 Digit Subnode address and 8-character device address.

11.3. Reports & Logs:

11.3.1. The system shall provide for the ability to generate reports based on system history.

11.3.2. The system shall allow the system operator to enter custom comments up to 255 characters for each event and have those comments recorded in the system's history file.

12. CONTROL ASPECTS OF SYSTEM SOFTWARE

- 12.1. The system shall provide for the direct control of all outputs associated with I/O (Input / Output dry contact relay) points on NIONs. In addition, the system shall have the ability to control and program a sub-system Notifier AFP-1010, AM-2020, or AFP-400 Fire Alarm Panel through a terminal mode window (ASCII terminal type connection) interface to microprocessor-based sub-systems via an RS 232 serial NION if available as an ancillary feature.
- 12.2. The system shall have the ability to control Notifier Fire Alarm Panels: AFP-200, AFC-600, and NFS-640.
- 12.3. Discrete I/O NION interfaces allow the system operator to initiate a change of state for the associated dry contacts.
- 12.4. A scheduling utility shall be included with the workstation to configure the I/O points on these NIONs for automated activate/deactivate, and Arm/Disarm (depending on device type) status.
- 12.5. The workstation shall provide configuration utilities for monitoring and control profiles. These profiles shall be user definable for distribution of monitoring and control allowances for operators per workstation.
- 12.6. Terminal mode interfaces using serial NIONs (if available for the specific system) shall be available to allow full programming and control of the system being monitored and shall provide the operator with the ability to take advantage of all features supported by a CRT attached to the associated individual sub-system.
- 12.7. Under no condition shall any sub-system be required to rely on the network for any data processing required to perform its particular function. Each individual sub-system shall be in effect "stand-alone" as to insure its continued operation should a disruption in communication with the UniNet™ system be experienced.

13. SYSTEM EXPANSION:

- 13.1. Additional software and hardware modules shall be currently available by the system manufacturer to provide for:
- 13.2. CCTV with on-screen Pan/Tilt/Zoom and live video on-screen.
 - 13.2.1. Supported systems shall include the following CCTV switch manufacturers, Javelin, Pelco, Burle/Phillips and Vicon. The ability to support all listed CCTV switch units simultaneously on the same system shall be supported.
- 13.3. Security and Card Access.
 - 13.3.1. The system shall consist of the UniGuard Access Control Application. The application shall permit full configuration and control of one or more NION-2DRN over a UniNet™ network in both wide- and local-area configurations).
 - 13.3.2. The UniGuard main screen shall display access-control-related events and general events as they appear in the system. Through this main screen, it shall be possible for any event to be selected for viewing extended information. If the event relates to a specific cardholder, that cardholder's information can be viewed as well.
 - 13.3.3. It shall be possible to provide control of any door or output point configured on a NION-2DRN, allowing locking and unlocking, activation of outputs, or pulse/momentary unlock operations.
 - 13.3.4. The application shall provide the ability to fully configure the NION-2DRN. Configuration options shall consist of ability to set up cardholders, time codes, access codes, time code groups, and holiday codes.
 - 13.3.5. Download

- 13.3.5.1. All configuration data shall be down loaded to the NION-2DRN and stored locally at each NION-2DRN for faster response times and independent operation.
- 13.3.5.2. Doors shall be configured using UniGuard software that allows definition of input points as request-to-exit points, keypads for PIN only or CARD PLUS PIN operation and the definition of output points as door contacts when monitoring door status. It shall also be possible to configure momentary open times, instant lock, and open and close times. Through these parameters, and the use of door supervision, the integrated UniGuard software within the NION-2DRN shall generate event status information about the door(s) including: door ajar, forced entry, anti-passback violation, and use of invalid card or PIN.
 - 13.3.5.2.1. It shall be possible for the user to create user-defined PIN (Personal Identification Numbers) or system (algorithm) defined PINs.
 - 13.3.5.2.2. When equipped with keypad readers, the system shall support silent duress alarm when the user selects a pre-defined key sequence.
- 13.3.6. Control and Monitoring
 - 13.3.6.1. It shall be possible to control the NION directly, or remotely through a UniNet™ network. The command and control options shall consist of:
 - 13.3.6.1.1. The ability to manage and control multiple NION-2DRNs at multiple locations.
 - 13.3.6.1.2. Graphical definition and configuration of time codes, time code groups, doors, door groups, access codes, holiday codes, and the card database.
 - 13.3.6.1.3. Control of anti-passback, anti-passback forgiveness, and facility code override.
 - 13.3.6.1.4. Configuration of card readers and doors, with options for various readers, locking options, REXs, (Request to Exit buttons) door contact inputs, and other related devices.
 - 13.3.6.1.5. Generation and annunciation of numerous events to indicate various normal and off-normal door states (using information from card readers, REXs, and door contacts).
 - 13.3.6.1.6. The ability to remotely control and configure one or more NION-2DRNs, including nodes over wide-area BCI networks.
 - 13.3.6.1.7. Definable operator accounts and access levels.
 - 13.3.6.1.8. Full control of all doors and output points.
 - 13.3.6.1.9. On-screen annunciation of all events, including the ability to view information about the event or cardholder.
 - 13.3.6.1.10. Logging of all events to history.
 - 13.3.6.1.11. Alarm annunciation from within the workstation application.
 - 13.3.6.1.12. Graphical interface to card access with support for up to 512 doors.
- 13.4. Incident Reporting Module.
 - 13.4.1. The IRM shall permit users to separately track information regarding incidents. Incidents may be derived from events automatically from the system, or may be generated manually by the user either from the host application or directly through the IRM interface client software.
 - 13.4.2. When an incident is created, its state shall remain open until the user manually closes the incident. While the incident is open, several operations may occur that require the user to update the information regarding the incident. It shall be possible the System Administrator to configure the information collected through

user-defined fields. As the event information is updated or a period of inactivity occurs, the IRM may change colors or utilize other visual cues to keep the user constantly updated regarding the incident, that it is currently active, or until the user closes the entry.

13.4.3. All data regarding incidents shall be stored within locally maintained databases, utilizing the information and fields as defined for display by the IRM. Reporting and reviewing the information shall be possible utilizing the History Manager or a combination of both. The IRM shall be configurable to run on a second, attached monitor concurrently with the host application using the dual monitor feature available within Microsoft Windows 98 or Windows 2000.

13.4.4. When employed, it shall be possible to display the IRM on a second monitor with the addition of a second video graphics adapter or dual-head card.

13.4.5. Software Operation

13.4.5.1. The IRM shall be constructed as an ADD-In application that communicates with a UniNet™ event manager software application. The IRM will automatically create incidents for a configurable set of events in the system. It shall also allow incidents to be generated manually, such as those based on phone or radio calls. It shall support multiple workstations, giving each workstation the capacity to view actions performed by other IRM stations. The software shall provide a real-time, multiple operator incident-handling system. The system shall be versatile enough to allow numerous custom defined fields for each incident, and allow both custom handling and color-coding for the incidents based on their status.

13.4.6. Security

13.4.6.1. The IRM shall depend on the system profile assignments for security access, including user name and profile information (if any).

13.4.7. Databases

13.4.7.1. The IRM shall implement and utilize the Microsoft Access database format, maintaining the ability to open and access multiple databases and/or tables concurrently. The main database of the IRM shall be centrally located.

13.5. Photo Imaging Client

13.5.1. The system shall support an integrated photo imaging software client known as UniBadge. It shall be possible to integrate the client software application at any time into the system. The system shall support the Fargo PRO series of Dye Sublimation direct to plastic badge printers.

13.5.2. The UniBadge application shall be used to create and print access control and identification badges using information stored in Microsoft Access databases. It shall be possible for the administrator to either create or import member information to be saved in the UniBadge member database or data source.

13.5.3. Badge templates can be created with text, photo, and barcode fields placed on them. Then, the corresponding information in the member database can be linked to those template fields via UniBadge data definitions. The system shall permit the operator to set up users, set up data definitions and set up data sources. When using data sources, the operator shall be able to choose fields to be used on badge templates.

13.5.4. It shall be possible for the operator to choose one or multiple badges for immediate printing, or for placement in a print queue for batch printing.

13.5.5. The following features shall be supported:

13.5.5.1. Graphical definition and configuration of users and profiles, badge templates, template groups, data definition fields, and data source configuration.

- 13.5.5.2. Ability to utilize member databases from the UniNet™2000 workstation or UniGuard™ Card Access application to use for badge printing.
- 13.5.5.3. Definable operator accounts and access levels.
- 13.5.5.4. Ability to link data definition fields on badge templates to fields in the data source database.
- 13.5.5.5. Complete control of badge template appearance, including use of static bitmap images, text and graphic fields using included graphics tools.
- 13.5.5.6. Ability to organize badge templates into groups.
- 13.5.6. Multiple Formats
 - 13.5.6.1. The system shall support multiple badge formats including portrait and landscape formats. All installed Windows fonts shall be supported and shall automatically resize point size to fit the defined badge field. Multiple industry standard bar code fonts shall also be supported
- 13.5.7. Database
 - 13.5.7.1. The system shall support connection to any system member database found on the system.
- 13.5.8. Badge Templates
 - 13.5.8.1. It shall be possible for the operator to define multiple badge formats for different departments. The Windows color palette shall be supported.
- 13.6. Guard Tour Client
 - 13.6.1. The Guard Tour Software application client shall facilitate security monitoring of a building complex by making use of any pre-selected series of existing UniNet™ monitoring points. It shall provide means for a human guard to electronically register his presence at various checkpoints. The software shall be designed to work with the UniNet™ network and either a workstation or the UniGuard card access application running in monitor mode.
 - 13.6.2. The system shall be specified as the UniTour software package as developed and supported by NOTIFIER©.
 - 13.6.3. It shall be possible for the system administration to create tours with checkpoints that utilize access devices, such as card readers, on the network. In addition, it shall be possible to organize tours into tour groups for random tour selection, so that the same checkpoint pattern will not always be followed.
 - 13.6.4. Within the main screen, guard tour related functions shall be displayed as they occur in the system. Through this screen, it shall be possible for any feature to be accessed for user, tour and group editing and monitoring. The main screen shall display details of the current running tour, as well as the list of defined tours and available groups. Configuration options shall be provided to set up operators, cardholders, time codes, holiday schedules and other related functions.
 - 13.6.5. The system shall permit guards to walk a defined pattern of checkpoints.
 - 13.6.6. The following features shall be available on the system:
 - 13.6.6.1. Ability to read various triggering actions, including card readers, key switch and manual contact closure input devices.
 - 13.6.6.2. A history log shall be maintained of all guard tour activity.
 - 13.6.6.3. Ability to generate reports of inspections and analyze data spanning multiple tours or guards using UniNet™2000 history manager.
 - 13.6.6.4. Real-time notification of tour status and any tour inconsistencies.
 - 13.6.6.5. Definable operator accounts and access levels.
 - 13.6.6.6. Graphical definition and configuration of users and profiles, tours, tour groups, tour schedules, and holiday schedules.
 - 13.6.6.7. The ability to pause, delay, or stop a tour in progress (with proper security access.)

- 13.6.6.8. On-screen annunciation of all events, including the ability to view network connection messages and off-normal checkpoint messages, such as a missed checkpoint.
- 13.6.6.9. Alarm annunciation from within the workstation application.
- 13.6.6.10. Importable monitor points (checkpoints) from existing workstation or UniGuard databases.

14. INSTALLATION:

- 14.1. All equipment and components shall be installed in strict compliance with manufacturers' recommendations. Consult the manufacturer's installation manuals for all wiring & fiber optic diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the riser/connection diagram for all specific system installation / termination / wiring data.
- 14.2. Conduit and Wire:
 - 14.2.1. Conduit:
 - 14.2.1.1. Conduit shall be in accordance with the National Electrical Code (NEC), local and state requirements.
 - 14.2.1.2. Where possible, all wiring & fiber optics shall be installed in conduit or raceway.
 - 14.2.1.3. Cable must be separated from any open conductors of power, or class 1 circuits, and shall not be placed in any conduit, junction box or raceway containing these conductors, as per NEC Article 760-29.
 - 14.2.1.4. All circuits shall be provided with transient suppression devices and the system shall be designed to permit simultaneous operation of all circuits without interference or loss of signals.
 - 14.2.1.5. Conduit shall not enter the control equipment, or any other remotely mounted control panel equipment or back-boxes, except where conduit entry is specified by the FACP manufacturer.
 - 14.2.2. Wire:
 - 14.2.2.1. All system wiring shall be new except as allowed herein and approved by the manufacturer for intended communications using Echelon's LonWorks.
 - 14.2.2.2. Wiring & fiber optics shall be in accordance with local, state and national codes (e.g., NEC Article 760) and as recommended by the manufacturer of the fire alarm system. Number and size of conductors & fiber optics shall be as recommended by the fire alarm system manufacturer.
 - 14.2.2.3. All wire and cable shall be listed and/or approved by a recognized testing agency for use with a protective signaling system except as specified herein.
 - 14.2.2.4. All communication wire to nodes or to computers shall consist of minimum manufacturer's recommendations and approved wire specification supporting speeds of 78Kps to 10mB/sec communications.
 - 14.2.3. Terminal Boxes, Junction Boxes and Cabinets:
 - 14.2.3.1. All boxes and cabinets shall be UL listed for their use and purpose.
 - 14.2.3.2. The PC based workstations shall be connected to a separate dedicated branch circuit, maximum 20 amperes. This circuit shall be labeled at the main power distribution panel as FACILITIES MONITORING SYSTEM. PC workstation power wiring shall be 12 AWG and grounded securely to either a cold water pipe or grounding rod. Where required, a UL listed 864 UPS system shall be provided.

15. SYSTEM SETUP & CONFIGURATION

- 15.1. Provide the services of a factory trained and authorized technician to perform all system software modifications, upgrades or changes. Field technicians shall be NICET Level 1 (minimum) certified.

- 15.2. The factory trained technician shall install initial data and artwork at each workstation including:
 - 15.2.1. Distribution of monitoring, control and security profiles as requested by owner.
 - 15.2.2. Area diagrams, floor plans, key maps and screen titles.
 - 15.2.3. Auto-navigation criteria.
 - 15.2.4. Guidance text as provided by owner.
 - 15.2.5. ".wav" files for custom voice annunciation as provided by owner.
16. FINAL INSPECTION:
 - 16.1. At the final inspection a factory trained representative of the manufacturer of the major equipment shall demonstrate that the system function properly in every respect.
17. INSTRUCTION/TRAINING:
 - 17.1. Provide instruction as required for operating the system. Hands on demonstrations of the operation of all system components and the entire system including user-level program changes and functions shall be provided. A factory trained and certified representative shall provide instruction.
18. WARRANTY:
 - 18.1. All work performed and all material and equipment furnished under this contract shall be free from defects and shall remain so for a period of at least one (1) year from the date of acceptance. The full cost of maintenance, labor and materials required to correct any defect during this one-year period shall be included in the submittal bid.
19. END OF SPECIFICATION.