INTEGRATED SOFTWARE TECHNOLOGIES INC.

VisiNet™

Network Management System

Users Manual

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 OVERVIEW

VisiNet™, IST's Flagship Network Management System (NMS) product, is currently in use by companies through the world to provide local and remote management capabilities of Satellite Communication networks of all sizes and architectures. VisiNet™ is a Native Microsoft Widows NT/2000 Product/Framework designed using the latest Object Oriented Programming (OOP) methodologies to provide superior reliability while achieving simplicity and reduced costs. Designed with the end user in mind, VisiNet's simplicity and intuitive user interface work together to provide one of the simplest NMS products in the industry to use. This translates into less required training and quicker product proficiency of customer personnel, helping to further reduce the TCO (Total Cost of Ownership).

VisiNet™ provides the user with a robust set of features similar to those found in Network Management Products offered by other venders. These features work to give the user all the tools necessary to effectively and efficiently manage the day to day operations of their satellite based network from device fault detection and management to performance evaluation and system configuration. Following is a list of basic features of the VisiNet™ product.

- Microsoft Standard Graphical User Interface
- Color Coded/Active Object Blinking Status Indication
- Selectable/Configurable Audible Alarms
- Data/Time Stamped Event Reporting and Logging to Industry Standard Relational Database
- Robust User Account Based Security System
- User Configurable Virtual Circuit Status Reporting
- Multiple Remote GUI Client Capability
- SNMP Device support
- Fully scalable architecture

VisiNet™ comes standard as a stand-alone local workstation located in close proximity to the earth station equipment being interfaced to, with optional remote capabilities provided via any TCP/IP based LAN/WAN communications infrastructure. The system provides real-time status and alarm notification and control capabilities of the devices connected to it. All alarms are reported to the user via a user selectable audible alarm and a visual indication while also being date and time stamped and logged to the system hard disk in the form of an industry standard relational Database file for archiving purposes.

1.2 WARRANTY

The system is warranted against NMS software errors for a period of one (1) year from the date of purchase. This warranty is limited only to software errors (bugs) of the NMS system itself and not to hardware or operating system problems. The warranty does not cover system problems that are the result of hardware or software problems of the devices being monitored and controlled. This includes any and all software and/or hardware revisions of the devices being controlled.

For warranty issues, please contact IST Inc. (480) 704-5066.

1.3 SYSTEM REQUIREMENTS

VisiNet™ is delivered as either a turnkey system on a computer that is approved for NMS operations, or as an installation media requiring the user to perform the system installation. In the later case, Visinet must be installed on a system meeting the required specification (see System Requirements) The installation, by the end user, of any software not directly related to the operation of the NMS will void all system warranties.

For users not purchasing VisiNet as a turnkey system (No Hardware), the following outlines the minimum required hardware set:

- Pentium III+ class PC with 128 Meg RAM minimum running Microsoft NT Workstation 4.0 (Service pack 5 or higher) or Win2000
- XGA Monitor with resolution set to 1024 x 768 and Fonts set to "Small Fonts"
- Multi-port serial I/O card if needed (with RS232 and RS 422/485 capabilities)
- Mouse, keyboard, floppy drive, audio card and speakers (required for Audible alarms)
- TCP/IP Networking services loaded and operating properly (IP Address can be selected by user or use 200.0.0.1)
- System Relational Database (for viewing the Event Log Data base files)

1.4 NMS SYSTEM LICENSE

VisiNet™ has been implemented with a License Control System (LCS) to guard against any unauthorized system duplication/multiuse, this section explains the LCS. The user, in purchasing VisiNet™, has purchased the right to use a single (or multiple copies of the system depending on the purchasing agreement) copy of the NMS. This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result is severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

The License Control System requires the use of a HW License Key supplied by the NMS manufacture for each Front End Processor (FEP) server unit (see System Architecture section for description of FEP). This Key my be either a USB type of Parallel Port Type and must be connected to the corresponding port (USB or Parallel) of the PC that is running the FEP server and device driver modules of the NMS. The Key must be connected prior to system startup and remain connected for the life of the NMS. The NMS will not function properly without the proper Key connected. Replacement of lost Keys will be at the discretion of the NMS manufacture and may require additional License costs. Damaged or malfunctioning Keys MUST be returned to the manufacture prior to replacement Keys being sent to customer.

1.5 INSTALLATION

VisiNet™ installation media is delivered with explicit instructions on the installation procedure in the form of a text file named Readme.txt or Install.txt. These instructions are also included as Appendix A. For operating system installation info, please refer to associated Microsoft documentation. For Installation Instructions of associated Hardware devices such as multi-port serial I/O modules see related hardware manufacture's documentation.

NOTE: Prior to installation connect the HW KEY delivered with the installation media to either the master NMS computer's parallel or USB port depending on the type of Key delivered.

NOTE: All VisiNet™ screens are designed to be displayed on a monitor with resolution set to 1024x768 and Font Size set to Small Fonts. For proper graphics display, make sure that the target computer's display properties are set to these values. These can be set via the "Settings" tab of the "Display Properties" dialog box. To open the "Display Properties" dialog box, select the "Display" option within the Window's Control Panel or simply place the mouse cursor anywhere on the Widows Desktop, click the right mouse button, and select the "Properties" option.

2.0 OVERVIEW

2.1 SYSTEM DESCRIPTION

VisiNet™ is a Native Microsoft Widows NT/2000 Network Management System Product/Framework designed using the latest Object Oriented Programming (OOP) methodologies that provides complete monitor and control capability for the various up-link and down-link subsystems present in a typical satellite earth station(s) or Satellite network such as VSAT applications. The NMS comes standard as a stand-alone local workstation located in close proximity to the earth station equipment being interfaced to, with optional remote capabilities provided via any TCP/IP based LAN/WAN communications infrastructure. The NMS is designed as a distributed multi-tier client/server based architecture that allows it to meet the requirements of many different network architectures and configurations by allowing different logical parts of the system to be located in many different geographical locations while in-turn allowing all these individual distributed elements to be integrated into a global application.

2.2 FEATURE SET

VisiNet™ provides the user with a robust set of features that work to give the user all the tools necessary to effectively and efficiently manage the day to day operations of their satellite based network from device fault detection and management to performance evaluation and system configuration. Following is an overview of the standard features provided by VisiNet™.

- **Platform.** VisiNet™ is delivered as a set of Native Microsoft Windows NT/2K applications leveraging the power and availability of COTS Software and Hardware.

- **Configuration.** VisiNet™ can be configured as a stand-alone system for small applications, or as a multi-server distributed system for the largest and most complicated of applications.

- **Remote Options.** Multiple Remote GUI Client access is standard, and supports all TCP/IP based LAN/WAN connectivity solutions.

- **Graphical User Interface (GUI).** The user interacts with the system by using a mouse to select different graphical objects and a keyboard for data entry. The **GUI** presents network elements to the user in the form of drawings and diagrams while utilizing colors to present the status of these different elements.

- **Audible/Visual Alarms.** All system alarms/faults are categorized as either Major or Minor, and presented to the user via Standard color coding: RED indicates a major alarm condition, YELLOW indicates a warning condition, and GREEN indicates an OK condition. The presence of an unacknowledged Alarm event is represented by active object blinking and user selectable audible alarm.

- **Device Control Security.** Access to Device Control capabilities is restricted on a user basis. Control access per user is Device based. Users can only issue Control Commands to devices they have been assigned access to by the Administrator..

- **Maintenance Mode.** Any device, or number of devices, in the system can be put into a maintenance mode, effectively removing the device(s) from the NMS polling cycle.

- **Event Reporting.** VisiNet™ provides a robust event reporting mechanism for logging Alarm, Control, and Runtime Data events. All three event types are Date and Time stamped and stored in separate industry standard relational databases (Event Logs). Viewing and printing capabilities are provided for each log. The Control Log

allows for event reconstruction and user accountability while the Runtime data log provides a means of performance analysis and data trending.

- **Virtual Circuits.** VisiNet™ allows the grouping of individual devices, and their related status values, into virtual circuits representing the overall status of all associated devices. This is useful for easier status tracking of complete circuit paths.

2.3 ARCHITECTURE

VisiNet™ is a Native Microsoft Widows NT/2000 Product/Framework designed using the latest Object Oriented Programming (OOP) methodologies to provide superior reliability while achieving simplicity and reduced costs. It is designed as a distributed multi-tier client/server based system allowing various elements of the system to be distributed among different PC processing units all communicating via the Open Standards of TCP/IP. This distributed capability allows the standard VisiNet™ product to be configured meet many different Network Architectures and/or system Performance requirements.

VisiNet™ multi-tiered architecture is comprised of three (3) separate processing subsystems (tiers), all integrated together to provide the complete end product. These subsystems are:

1. Graphical User Interface (GUI)
2. Front End Processor (FEP)
3. Device Drivers

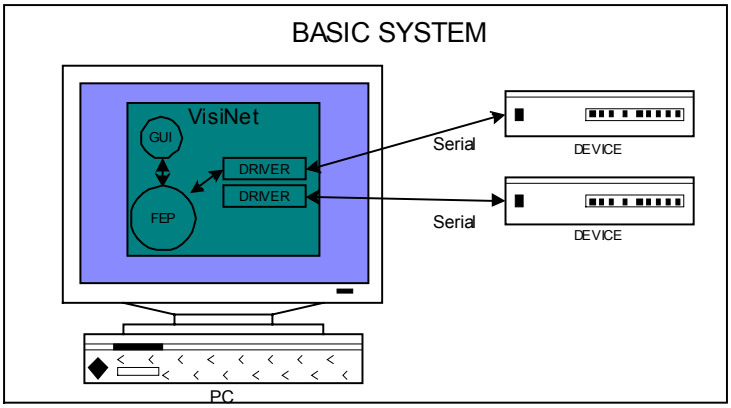
The Graphical User Interface (GUI) is the portion of the system that the user(s) visually see and interact with. It comprises all the user interface features and capabilities such as device management, fault management, security management, and event reporting. As far as the general user is concerned, this is the VisiNet™ product.

The Device Drivers are the individual backend processes/elements that communicate with all the physical devices to be managed by the system such as modems, converters, and amplifiers. These elements handle all the aspects of polling the devices for data, sending this data to any connected GUI clients on an exception base and relaying a user commands received from any connected GUI clients to the device(s). All device drivers are custom designed to interface directly with a specific target device. This ensures that all device drivers have been optimized for performance and reliability to a level that cannot be achieved by generic device drivers. Furthermore, because the NMS is designed as a distributed system with each device driver acting as an individual software module, problems that might occur in one device driver cannot affect the performance or operation of the rest of the NMS.

The Front End Processor (FEP) is the server subsystem that connects the Device Drivers to the GUI(s). It acts as a middle-ware component providing both client and server features to both the GUI and the Device Drivers. It can be considered the Glue that holds the entire system together.

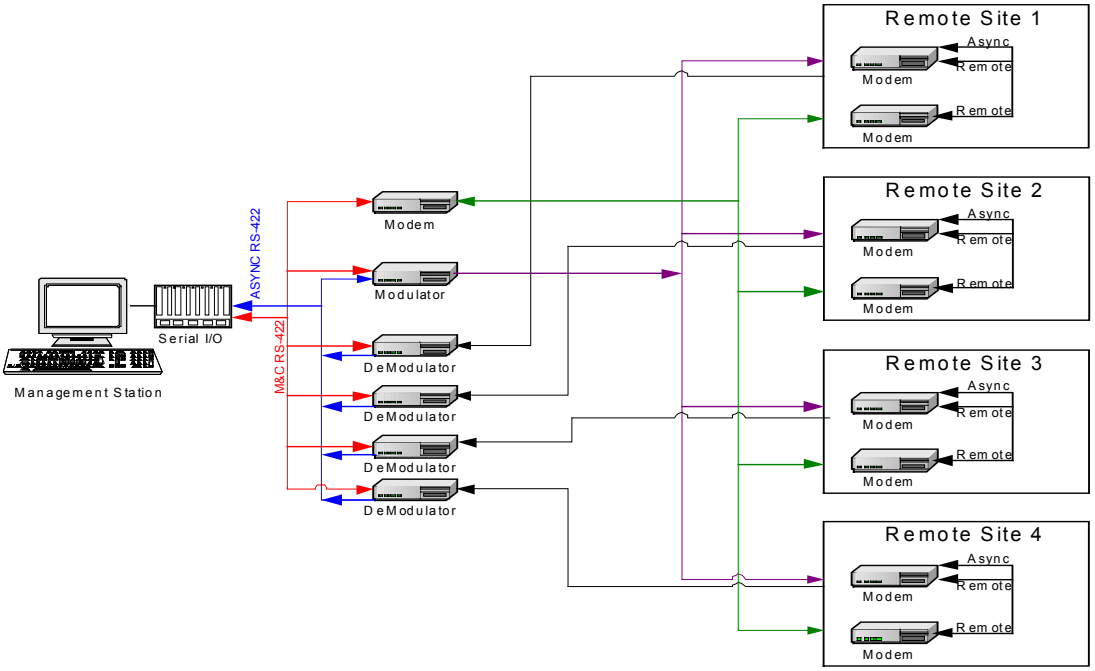
See Figure 2.1 for a general system architecture diagram.

Figure 2.1 Basic System



The distributed capabilities of the system are achieved be implementing the GUI/FEP interface via Standard Open TCP/IP protocols. This allows the GUI and FEP to be physically located on different machines communicating via a TCP/IP based network infrastructure. Furthermore, The FEP can service many GUI clients concurrently, allowing for multiple remote GUI clients to be run from various locations throughout a TCP/IP based network infrastructure. In turn, a GUI client can be connected to any number of individual FEPs concurrently. This architecture allows for virtually any combination of system elements (GUIs and FEPs) resulting in virtually unlimited overall system configurations based on the Standard VisiNet™ Product/Framework. Figure 2.2 provides a sample system diagram for a basic VSAT type of application.

Figure 2.2 Sample VSAT Application



2.4 USER INTERFACE

The system's user interface, termed Graphical User Interface (GUI), or Man Machine Interface (MMI), has been designed to be consistent with standard Microsoft Windows applications. The user interacts with the system by using a mouse to select different graphical objects and a keyboard for data entry. The MMI presents system elements to the user in the form of Icons, diagrams, and drawings, while utilizing colors to present the status of these different elements. Standard color coding is as follows:

- GREEN indicates an OK condition
- YELLOW indicates a Warning/Minor Alarm condition
- RED indicates a Major alarm condition
- PURPLE indicates an Invalid Fault Status condition.
- ORANGE indicates a Maintenance Mode Status condition.

This status color indicates the internally generated summary status state of all system devices associated with the graphical element in question. Status states are prioritized with Major Alarm having the highest priority, followed by Minor Alarm, followed by Maintenance Mode, followed by Invalid Fault State, , followed by OK condition. Therefore, if a graphical element is associated with a number of different devices, its color will indicate the highest priority status state of all the associated devices. For example, If an Icon represents a number of different devices, and one of the devices currently has a Major Alarm condition and one has a Minor Alarm condition and the rest have no Fault conditions (OK condition), the color of the Icon will be RED indicating the presence of a Major Alarm condition in one of the associated devices. Should the device with the Major Alarm condition transition to an OK condition, The color of the Icon will then be YELLOW indicating the presence of a Minor Alarm condition in one of the associated devices.

The presence of an unacknowledged event is represented by active object blinking. This system of objects, colors, and blinking provides for a very intuitive interface, regardless of the complexity of the system being monitored.

All customer equipment being monitored is represented in VisiNet™ by graphical objects. These objects are precise drawings of the equipment's front panel. In some cases, all actual front panel indications such as status LED's are present on the graphical object and react in real-time to the device. This high level of graphics provides the user with a very comfortable and non-intimidating environment.

2.5 STATUS INDICATIONS

Visual indications are comprised of the above mentioned color-coded status indication mechanism. Every ICON in the system displays the status of all associated devices using this color-coded status indication mechanism. In addition to color-coding, Icons represent the present of an unacknowledged event by blinking the current status color. These alarm indications are propagated up through all screens in the system from the lowest level Device Screen to the Main System Screen. This ensures quick and effective alarm interrogation by system personal.

Audible indications are comprised of the playing of a .WAV file upon receipt of an alarm set event. This audible will remain active until a user acknowledges the alarm. The Supervisor Account can disable this audible if desired. The default .WAV file can be replace with a custom sound if desired.

In addition to the Visual and Audible alarm indications mentioned, the system provides a number of different ways to view:

- a history of all alarm events
- only current system wide unacknowledged events
- only current device specific alarms

Other Alarm Indication, such as automated E-Mail notifications and automated personal paging, are possible and treated as add on options to the Standard VisiNet system.

2.6 EVENT REPORTING

VisiNet provides three types of event reporting capabilities, Alarm, Control, and Runtime data. All three data log event types are Date and Time stamped and stored in separate relational databases. From within the VisiNet™ GUI, the last 100 most recent events from each data log can be viewed in the respective Alarms Log, Controls Log, and Runtime data Log windows. For generating reports and full inspection of each data log, each data log must be opened and manipulated from within the target Relational Database Software Product, providing the user unlimited report generation capabilities. This allows Event Log inspection and report generation via a user preferred Database Management System.

Alarm Events:
All system alarm set and clear events are date and time stamped and stored in the Alarms data log database. For systems with an audio card, an audible alarm can be enabled to sound upon the receipt of an alarm condition. This audible alarm will remain active until a user acknowledges it.

Control Events:
All attempted user initiated system device control events are date and time stamped and stored in the Controls data log database. Along with the date and time stamp, the control event also logs the user name of the user that was logged into the NMS at the time the control event was initiated, a description of the event including the target device and point name, and the value that related point was set to.

Runtime Data Events:
The system also provides a runtime data logging feature for logging system device data point values to the Runtime data log relational base. The Runtime data log contains all the Runtime data events, with each event containing information on the source device, data point and new value. Control of Runtime data logging is provided on user selectable individual point basis and a delta trigger value or time interval. A Runtime data event will be logged for each Runtime logging enabled device data point when the value of the data point changes by a value greater than the user selectable Delta trigger value, or at the user selectable time interval. Each data point in the system can be individually enabled for Runtime data logging and has a user selectable unique Delta trigger value or logging time interval.

2.7 SECURITY

VisiNet provides system security on a user account basis. This security mechanism protects against unauthorized access to the controls of the devices managed by the system and is designated Device Control Access (DCA) protection. Users are assigned a User ID and Password by the System Supervisor and can manage their own passwords. The supervisor can add new users and delete old users from the system while also controlling DCA per user on a per device

basis. System control capabilities for each device in the system are only active while a valid user with access rights to the device is logged on to the system. Furthermore, all user activity is account activity is recorded and logged to the Controls Event Log. This provides user accountability and allows for event reconstruction. Furthermore, the supervisor has the capability to disable the DCA system resulting in an open unprotected system.

3.0 SETUP

3.1 COMPUTER SYSTEM BASICS

VisiNet is designed to run under the Windows NT or 2K Operating Systems (OS). Once the OS has finished loading, the user will be presented a Windows logon screen. This screen will prompt the user to type the CTL ALT DEL key sequence to logon to the system. After this key sequence has been typed the user will then be prompted with a login prompt asking for a user name and password. For systems that are delivered as turnkey systems (NMS software pre-installed and configured on vender delivered computer system), the computer is delivered with a default account set up with the following User name and Password.

USERNAME = "Administrator"
PASSWORD = blank (no password set

Once a valid user name and password has been entered, that user will now be logged onto the system. For various Windows administration tasks please see the related Microsoft documentation.

After logging on, the NMS may be started by double clicking, via the mouse, on the NMS shortcut icon. To add NMS capability to other user accounts, add a shortcut with the same properties as the NMS shortcut in the Administrator account.

NOTE: To power down the computer system, always shut down the system using the proper NT shutdown sequence. **NEVER SIMPLY JUST TURN OFF THE POWER OF THE COMPUTER**. This could result in the damage of certain Operating System files required for proper operation. Furthermore, it is a good practice to create multiple Windows NT Emergency Repair disks ERD. These disks can be used to repair possible Operation Systems problems in the future. For more information on ERD please see the related Microsoft documentation.

3.2 SYSTEM DIRECTORY AND FILE STRUCTURE

VisiNet is required to run on the physical hard drive labeled "C". The C drive must contain the required directory structure and all the NMS files. All the NMS files are located in a directory called "Visinet" off the C drive. This directory contains four sub-directories as follows:

1. "Drivers"
2. "Fep"
3. "Gui"
4. "Runtime"

Drivers directory:
This directory contains a directory for each device driver of the NMS. Each one of these directories contains three (3) files, a driver executable "**XXX Driver.exe**" that must be present in the respective directory for the system to be operational, a driver configuration "**DriverCfg.txt**" file that defines the communication specifics for the respective driver, and a driver debug file "**Debug.txt**" that contains any possible debug information should the respective driver encounter problems. The first 2 files must be present for the system to operate. The debug file is created by the driver upon startup.

Drivers are the elements of the NMS that talk over the computer serial ports to the various electronic subsystems. For specific directories that are present for this particular system please refer to Appendix C:

Driver Configuration Files are text files that contain communication configuration information for the driver located in the same directory. This file MUST be present and contain the proper information in the proper format for the respective driver to operate. Each driver requires a unique Driver Configuration file that contains configuration information specific for that particular driver. These files should NOT be edited by anyone other that IST personnel unless directed by IST. A sample configuration file follows:

```
**********************************************************************
*******
**                        Tx Combiner Driver Configuration File
**
**********************************************************************
**
<>
Driver Type = 1
Driver=1
Com Port=1,9600,N,8,1,2000,0
<>
```

Any line that contains a "*" as the first character is treated as a comment and is ignored.
Once the first Non-comment line is encountered, NO MORE COMMENTS CAN BE PRESENT.

The First Non-comment line defines the driver type and is used internally to control the Driver's configuration.

The Second Non-comment line defines the FEP interface channel that the driver will be mapped to.

The Third Non-comment line defines the properties of the MS Windows Com Port that the driver will communicate through and must follow the format of Com Port=a,b,c,d,e,f where:

- a = Com Port Number
- b = BAUD Rate
- c = Parity (N=None, E=Even, O=Odd)
- d = Data Byte Size
- e = Number of stop bits
- f = Polling timeout value in ms
- g = Polling cycle delay time in ms

Other line may follow depending on the Driver.

GUI directory:
This directory contains the actual Graphical User Interface (GUI) executable, all audio files (.wav files) needed by the system including the "alarm.wav", the GUI Debug error log file

"Debug.txt", and the "System" directory that contains all the required GUI configuration files. The GUI executable is what the user interacts with and is the bulk of the NMS. The "**alarm .wav**" file is the actual file used for the audible alarm and must be present in this directory for the audible alarms to work.

Runtime directory:
This directory contains various files required by the NMS including all the system Microsoft Access Database event log files and any corresponding event log archive database files (see section on Event Logging for details on the Event Logging capabilities and the related files.

FEP Directory:
This directory contains the systems Front End Processor executable (FEP.exe), and support files, which allows all the systems drivers to communicate with the GUI portion of the system and vice versa. The "FEPCfg.txt" file is the configuration file for the FEP executable and is used much like the driver configuration files.

3.3 SYSTEM STARTUP

To start VisiNet, run the "Visinet.exe" executable located in the GUI sub-directory of the Visinet directory on the C drive. This will launch the NMS application and all required components. The GUI will take approximately 5 sec to come up. During this initial 5 sec, all the device drivers are being started one by one, as is visible at the bottom of the Widows Desktop. Once all the drivers have stated, the main subsystem window will be displayed.

4.0 USER INTERFACE

4.1 OVERVIEW

The GUI consists of a vast number of widows. These windows are categorized into two types:

- Network Windows
- Feature Windows

Network windows are windows that present views of that actual network that is being managed. Feature windows are all the other windows in the system that the user interacts with to perform certain actions or operate different features, such as viewing Event Logs or changing a password.

The GUI presents the user with a hierarchical graphical representation of the entire network via Network windows. This visual hierarchy consists of four types of Windows:

- The Main Window
- Subsystem Windows
- Device Windows
- Device Faults Windows

The Main window represents the Highest level, or Global, view of the network and provides the user with the starting point with which to navigate to all network subsystems and devices. Device windows represent the Lowest level views while Subsystem Windows represent all intermediate level views. Users navigate the network by selecting different Icons representing different Subsystems and Devices resulting in the associated Subsystem or Device Windows to be shown. This graphical structure achieves a result much like using the Microsoft explore to navigate all the directories, subdirectories, and files on a hard-disk.

All Network windows follow basic Microsoft format standards. Each window has three (3) major components:

Title Bar:
Located at the very top of the window and contains the title of the particular window.

Menu Bar:
Located directly under the Title Bar and contains various user selectable menus that perform different actions.

Workspace:
The rest of the window where all system information is displayed.

4.2 MAIN WINDOW

The main window of the NMS contains a graphical representation of the system with Icons for all subsystems and/or devices connected to the NMS with the status of each individual subsystem and/or Device indicated by the background color of each Icon. The Main window is unique in that is contains all the supervisor operations and user account functions in the menu at the top of the window. There are seven (7) menu selections:

Shutdown:
Used to shut down the NMS system. If selected, the user will be prompted to acknowledge the request to shut down the system. If the GUI is running on a Master computer (the computer that is running the FEP and all Drivers), this selection will also shut down all the device drivers running on the computer.

Users:
Used to log onto and log off of the NMS system and to change passwords.

Supervisor:
Enabled only when the current user logged onto the NMS is the Supervisor, or has been assigned Supervisor privileges. Used to gain access to all Security and virtual circuit related configuration options

System:
Used to gain access to the System Preferences window which has two sections, General and Supervisor. The General section contains check boxes for Audible Alarms, Runtime Logging and Timed Control Events. These check boxes are used to Globally enable/disable the above mentioned features. The Supervisor section is used the enable/disable the Device Control Access (DCA) protection mechanism and modify the system's visual Refresh rate.

View: **
Used to select the various Event Logs (Alarm, Runtime, Controls, Unacknowledged Alarms, and Timed Control Events) to view and view Virtual Circuits Info Window. Each Event Log window presents the user with a copy of the last 100 Events for that particular Event Log that and have been logged to the corresponding Event Log Data Base since the NMS had been started, or since the Clear option had been selected. This window does not affect the actual Event Log Data Base and is designed to be a quick way to check on recent Event Activity.

Ack Alarms**
Used to acknowledge all alarms. This will stop all audible and visible unacknowledged alarm event indications

About:
Brings up window with version and copyright information.

** indicates menu item is used in other windows also

4.3 SUBSYSTEM WINDOWS

Subsystem windows contain graphical representations of individual subsystem in the system with Icons for all related subsystems and/or devices, with the status of each individual subsystem and/or Device indicated by the background color of each Icon. All Subsystem Windows contain four (4) menu selections:

Back:
Closes the current window resulting in the previous window in the network hierarchy being shown.

Home:
Closes all Windows and returns to the Main Window.

AckAlarms:
Same as Main Window.

View:
Same as Main Window.

4.4 DEVICE WINDOWS

Device windows contain graphical representations of the actual devices, including the values of all the data points of the device being monitored, and provide access to all the Controls of the device. Device windows also provide access to the different device related features such as configuration of Runtime Data Logging for the Device and Configuration of all Fault Data points for the device. The background color of the window indicate the current Status of the device. See Figure 4.1 for a sample Device Window. All Device Windows contain six (6) menu selections:

Back:
Closes the current window resulting in the previous window in the network hierarchy being shown.

Home:
Closes all Windows and returns to the Main Window.

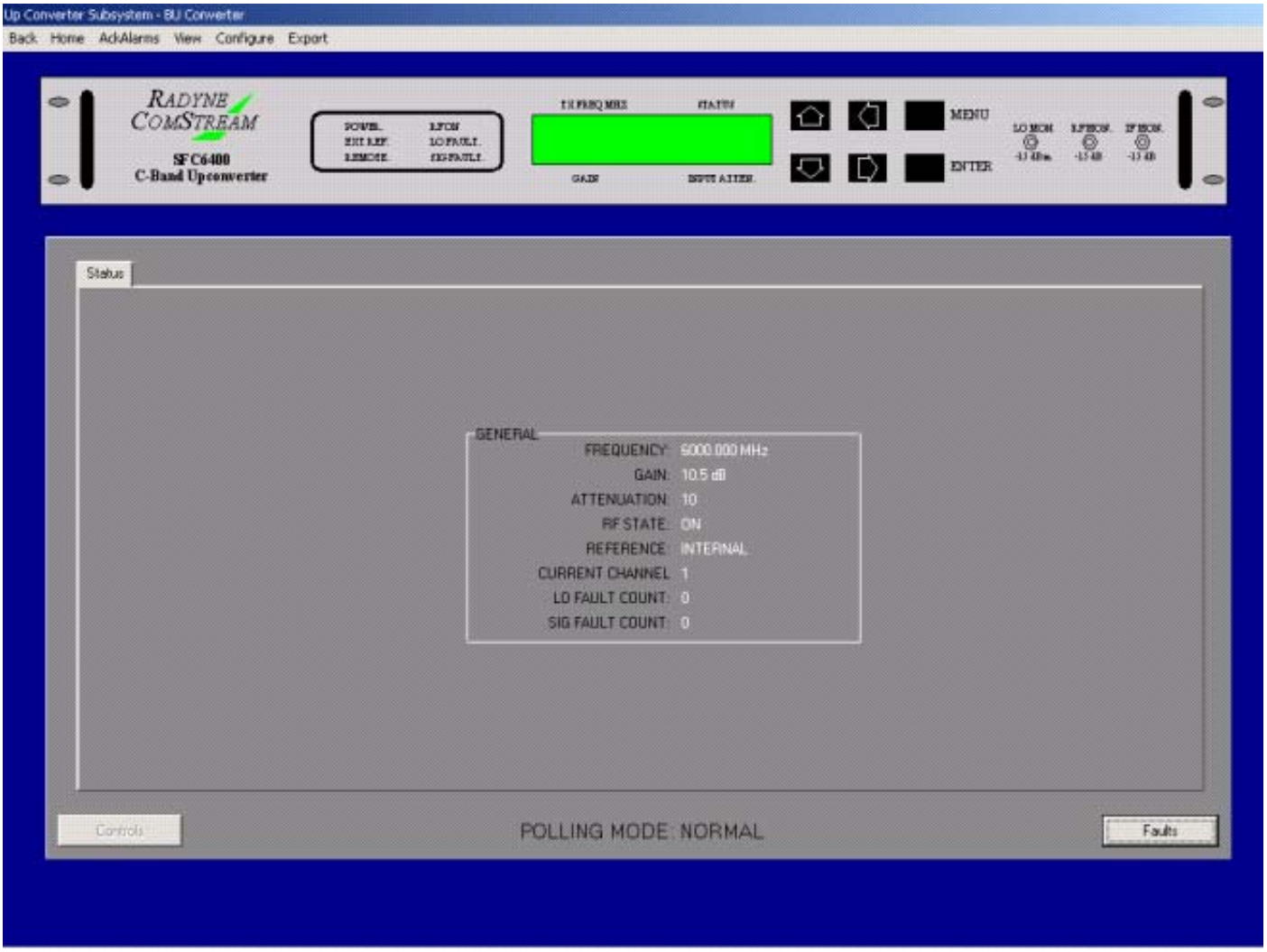
AckAlarms:
Same as Main Window.

View:
Same as Main Window.

Configure:
Used to gain access to the Runtime Data Logging control and Fault info configuration windows for the device.

Export:
Used to export the current values of all Data and Fault points of the device to a standard Text file.

Figure 4.1 Sample Device Window



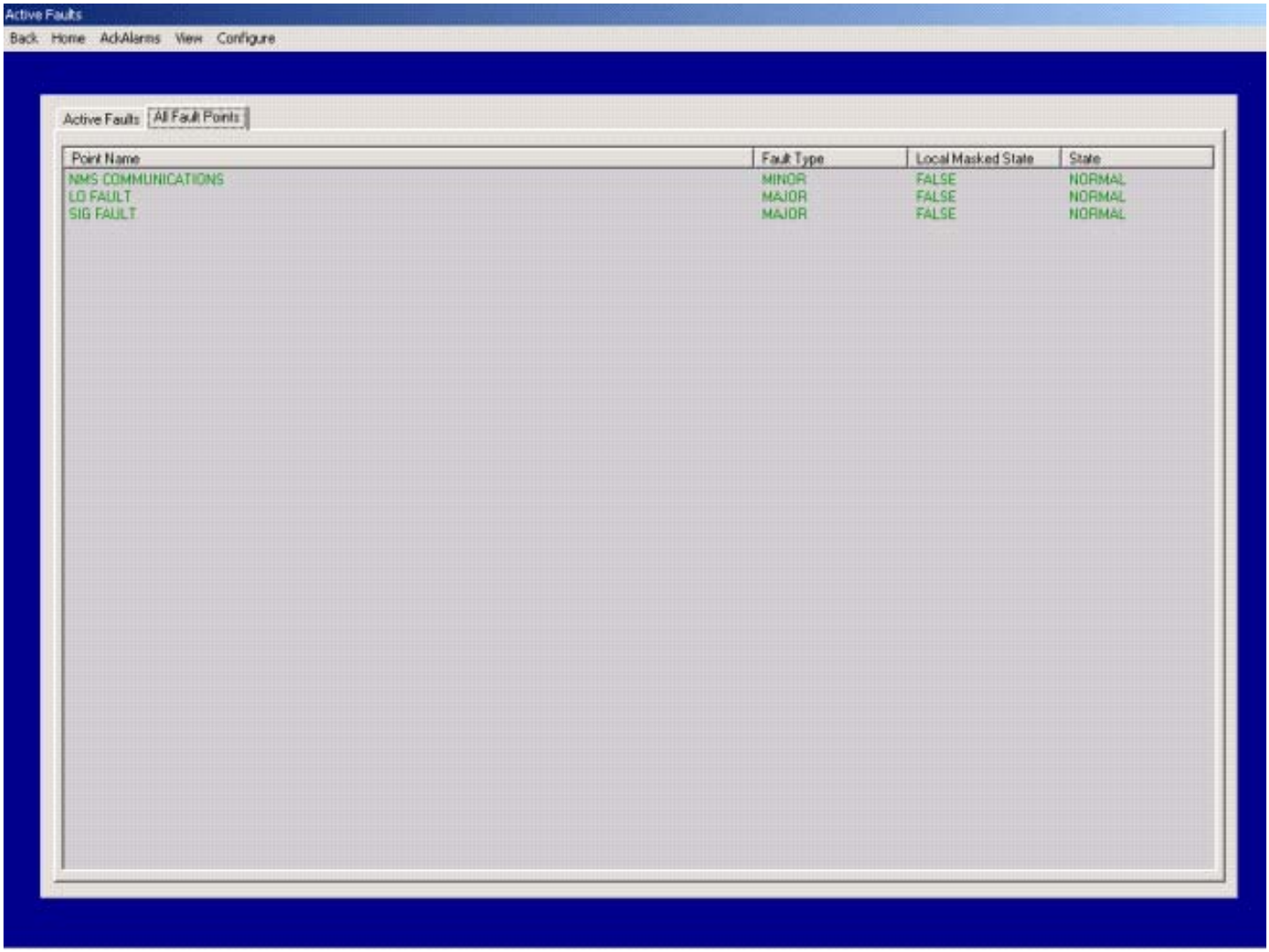
Window Elements

Element	Description
Controls Button	Provides access to all device Control functions
Faults Button	Opens the Device Faults Window for the device
Polling Mode Field	Shows the current Polling state of the device.

4.5 DEVICE FAULTS WINDOWS

Device Faults windows contain all the Fault status points of the actual devices in the system. The "Active" Tab show all device fault points that are currently Faulted, while the "ALL Fault Points" Tab shows the current status, Type, and Local Masked State of every fault point for the device. The background color of the window indicate the current Status of the device. See Figure 4.2 for a sample Device Faults Window. All Device Fault Windows contain the same menu selections as Device Windows excluding the "Export" Item:

Figure 4.2 Sample Device Faults Window



Window Elements

Element	Description
Active Faults Tab	Shows all currently active Faults
All Faults Points Tab	Opens the Device Faults Window for the device
Polling Mode Field	Shows the current status, Type, and Local Masked State of every fault point for the device.

4.6 EVENT LOG WINDOWS

The three Event Log Windows,

1) Alarms

2) Controls
3) Runtime Data

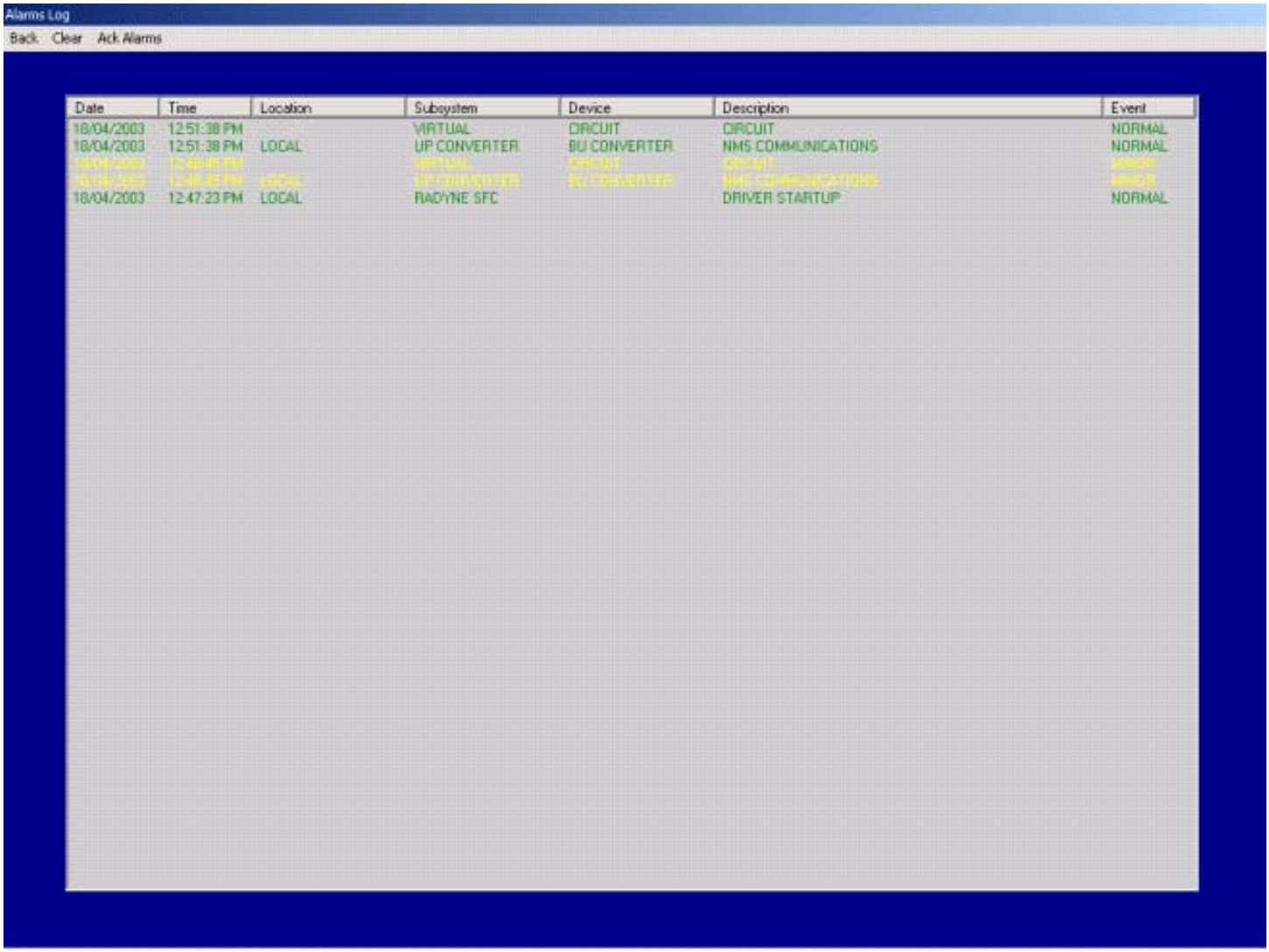
show last 100 most recently logged events by the respective Event Reporting Subsystems. See Figure 4.3 for a sample Alarms Log Window. All Event Log Windows contain three (3) menu selections:

Back:
Closes the current window resulting in the previous window in the network hierarchy being shown.

Clear:
Clears the list.
Note: This has no effect on the actual Event Log Database files.

AckAlarms:
Same as Main Window.

Figure 4.3 Sample Alarms Log Window

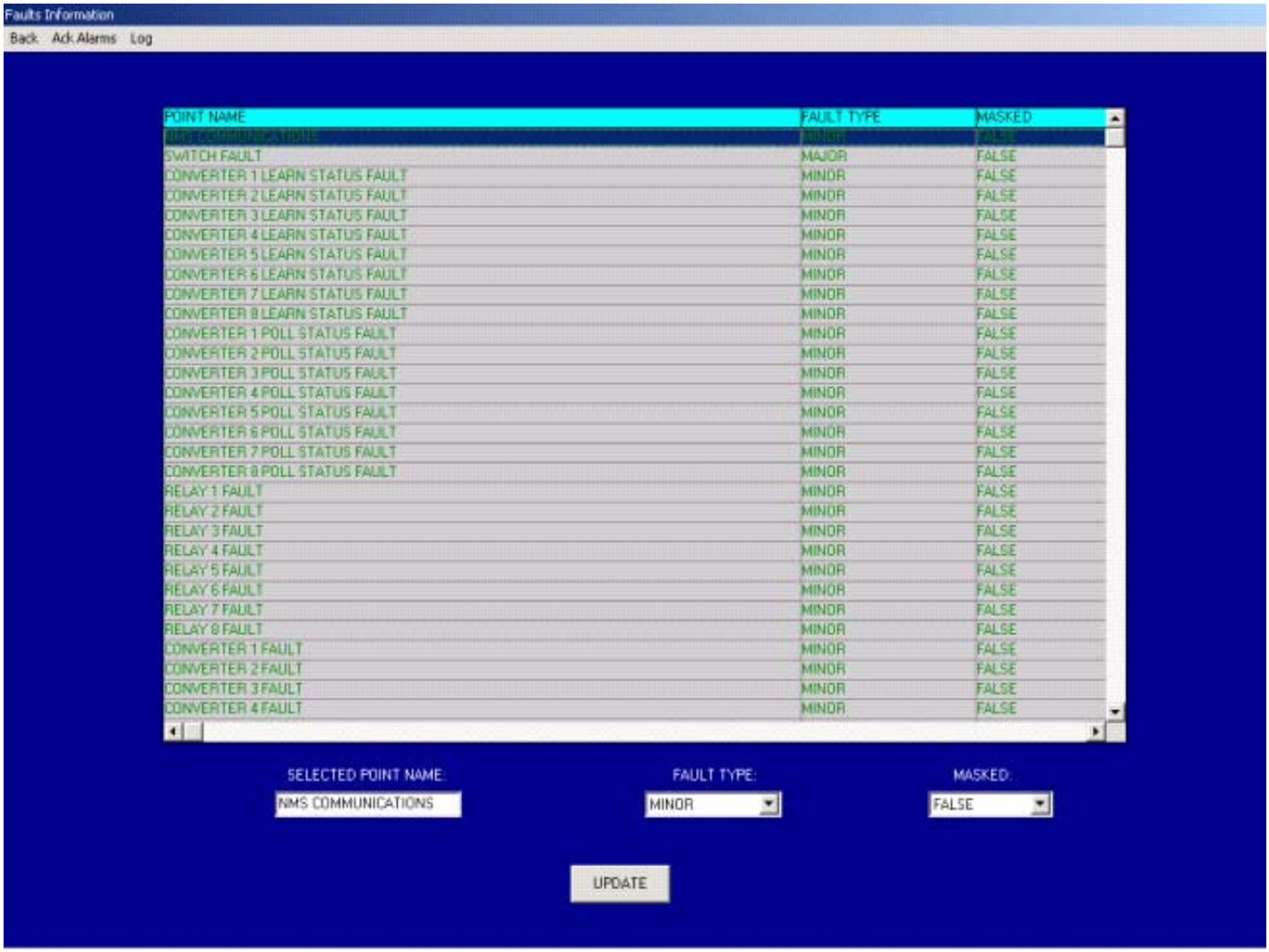


5.0 FAULTS CONFIGURATION

5.1 OVERVIEW

VisiNet allows the user to configure the type of each Fault, Major or Minor, for each device in the system, while also allowing the user to locally Mask each Fault for each device. This is handled using the Faults Info Window, accessible via the "Configure" Menu item in each Device Window and Device Faults Window (See Figure 5.1)

Figure 5.1 Faults Info Window



To modify a Fault Point:

1) Select the desired point from the list
2) Select the desired Fault Type and Masked values from the respective fields
3) Select the Update Button

6.0 SECURITY

6.1 OVERVIEW

VisiNet provides a robust security mechanism based upon user accounts to limit access to certain system features/settings, and to protect against unauthorized access to the controls of the devices managed by the system. Each User account is assigned an access priority and a Device Control Access (DCA) structure. The access priority specifies the type of user for the account, SUPERVISOR OR USER, and is used to limit access to certain system features/settings. The DCA structure controls the user's access to the commands capabilities for the individual devices in the system. The DCA mechanism can be disabled by a SUPERVISOR type user, resulting in an open system without any access control over the commands capabilities for the individual devices in the system. The system has a special built in SUPERVISOR account that has special privileges and is always present. This account is created the first time that VisiNet is run and is assigned a password of "SUPERVISOR". It is recommended that this password be changed once the system is running to ensure security integrity.

All user accounts are assigned one of two access priorities:

- SUPERVISOR
- USER

Users assigned USER priority can manage their own account password and have DCA as defined in the DCA structure.

Users assigned SUPERVISOR priority have the same DCA capabilities as USER level accounts but can also manage all User account functions such as adding new users to the system, deleting existing user from the system, and modifying existing accounts including, the DCA structure for each account. Furthermore, a SUPERVISOR level user has the capability to disable the DCA system resulting in an open unprotected system.

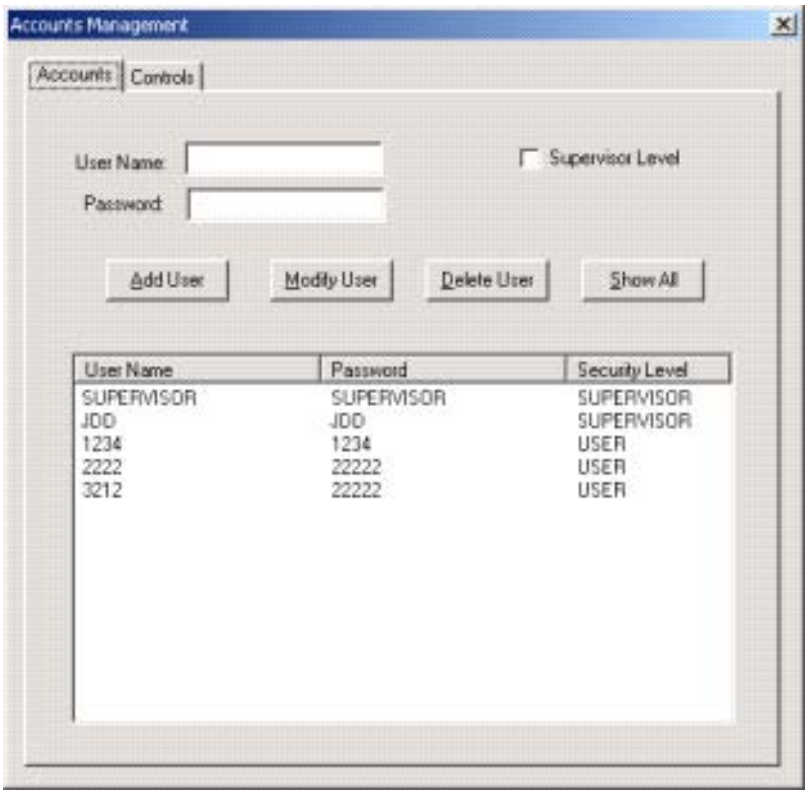
The DCA system controls what devices in the system a user has control access to. This is handled on a Per-User Per-Device basis. Each user can be assigned Control Access to any and all devices in the system. This provides unlimited control over individual user device control access.

6.2 ACCOUNT MANAGEMENT

All account management is performed via the Accounts Manager that is accessed by the Supervisor->Accounts Management menu on the Main Window. The Accounts Manager contains a section that handles account management and a section that handles DCA. The account management section is located on the Accounts tab while the DCA management section is located on the Controls Tab.

The Accounts tab in the Accounts Manager is used to create new accounts, modify and delete existing accounts, and view all accounts. All existing accounts are visible in the explorer like list box a the bottom. See Figure 6.1.

Figure 6.1 Accounts Manager Account Editor



To add a new account:

1) Enter a user name for the account in the User Name field
2) Enter a password for the account in the Password field
3) Select or de-select the Supervisor Level check box to control the account type
4) Select the Add User button.

To delete an existing account:

1) Enter the user Name for the account or select the account from the existing account list
2) Select the Delete User button

To modify an existing account:

1) Enter the user name for the account or select the account from the existing account list
2) Change the password if desired
3) Change the Supervisor Level check box if desired
4) Select the Modify User button

To view all existing accounts:

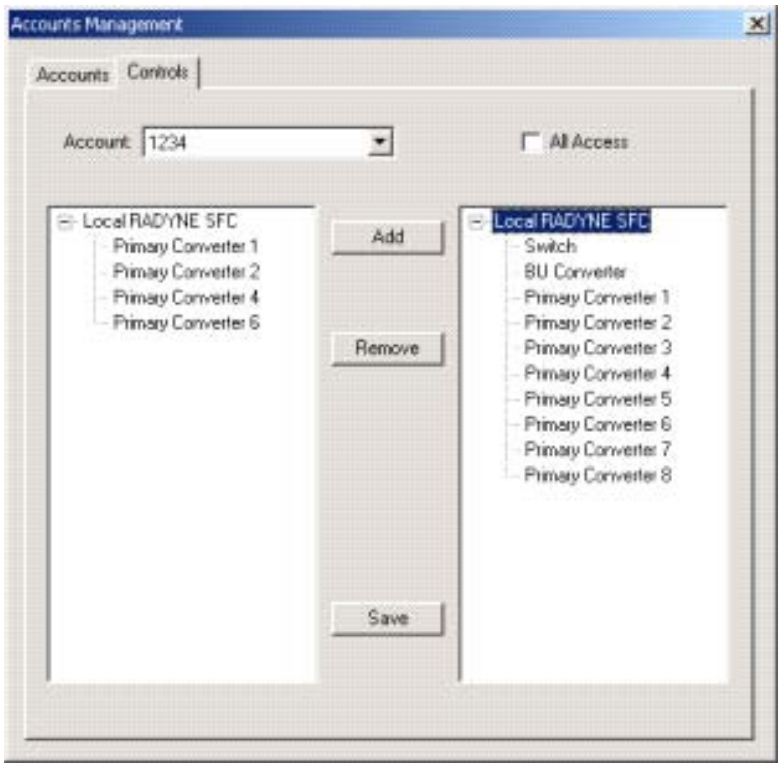
1) Select the Show All button

6.3 DEVICE CONTROL ACCESS MANAGEMENT

The Controls tab in the Accounts Manager is used to manage the DCA for all accounts. The list on the right side shows all the devices in the system while the list on the left side show all the

devices the selected account has control access to (DCA). For each account, DCA can be set to All Access, giving the account control access to all devices in the system or to individual device access giving the account control access to only the device desired. See Figure 6.2.

Figure 6.2 Accounts Manager DCA Editor



To set the DCA for an account:

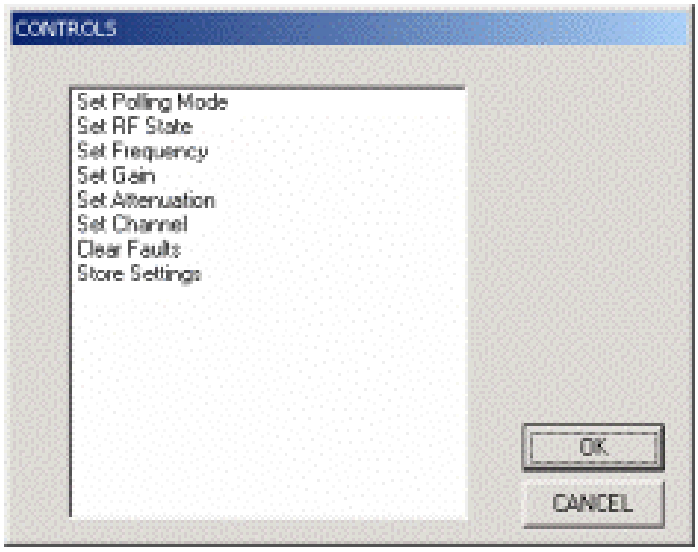
1) Select the desired account from the Account drop down selection box.
2) To provide All Access, select the All Access check box
3) To provide limited access, select the desired devices from the list on the left side then select the Add button. Continue this step until the desired devices are present in the list on the left side.
4) Once all DCA editing is complete for all accounts, select the Save button to save the setting to the hard disk.

7.0 SYSTEM CONTROLS

7.1 OVERVIEW

VisiNet allows users to change various parameters of the devices being interfaced to, provided that a user with proper DCA is currently logged onto the NMS. Devices present in the DCA for the current user will allow access to all the controls of the device. Devices not in the DCA for the current user will have access to the device's controls disabled. The number and type of parameters that are controllable vary from system to system and device to device. The ability to change parameters is provided on the individual Device screens via buttons labeled "Controls" and/or various buttons layered on the Device front panel graphic. When a "Controls" button is present, this button gives access to all the possible data elements that can be modified by the NMS for the particular device (See Figure 7.1). Selecting one of the items in the presented list, via either a double mouse click on the desired item or a single mouse click on the item followed by selecting the OK button, results in the control box for that data item being presented to the user. The user can then select an option or enter new data, depending on the type of data, followed by selecting the OK button to control the particulate device. Whenever possible, if the device in question rejects a command, say for invalid data, the user will be prompted with a message box indicating that the command failed. This is a very rare occurrence due to the level of data validation that is present in the system. However, should this occur constantly when trying to control a particular data point, refer to the device's user manual or contact IST Inc. to find out what why the data entered is invalid. Usually, this is the result of trying to enter a value for a data item that is invalid for the current operation mode the device is in.

Figure 7.1 Sample Controls Selection Dialog



8.0 EVENT REPORTING

8.1 OVERVIEW

The Event Reporting/Logging capabilities of VisiNet are provided by three Event Reporting Subsystems. Each subsystem handles a particular type of event, and operates independently from the other two subsystems. These subsystems provide three types of event reporting capabilities,

1) Alarm
2) Control
3) Runtime data.

Each Event Reporting Subsystem creates Events, logs/stores these Events to separate individual Event Log relational databases files for archiving, and sends the Events to the related Event Log Windows where the last 100 most recent events can be viewed. All of the Event Log database files are located in the "NMS/Runtime" directory and have the following names:

1) "Runtime Log.mdb"
2) "Commands Log.mdb"
3) "Alarms Log.mdb"

These files are the actual Relational Database files the NMS interacts with. To prevent against any system performance degradation due to excessively large Event Logs, the NMS limits the size of each type of Event Log to a fixed value and incorporates an archiving process should any of the Event Logs reach this size. This archiving process works as follows. As each event is logged to one of the three Event Logs, the size of the log is looked at. If the size of the log has reached the max allowed size, the NMS will rename the current log file to "*log name* Overflow 1.mdb" (where *log name* is the name of the type of log in question Runtime, Commands, or Alarms) and start logging alarms to a new "*log name* Log.mdb" file. Should the new log file also reach the maximum size, the NMS will rename it "*log name* Overflow 2.mdb" and start once again logging alarms to a new "*log name* Log.mdb" file. The NMS will continue on with this strategy until Log Overflow 4 has been filled. Once this happens the system prompts the user that all log files are full and that they should be saved before they are automatically deleted. If the log file reaches the maximum size and Overflow 1 through Overflow 4 exist, the system will delete all overflow files and start the whole archiving process from scratch. The number of events in an Event Log that has reached the Max size differs between the three different Event Logs but averages around 2,500. So an Event Log that has been archived 4 times, producing Overflow 1 through 4, will have approximately 10,000 events stored in the 4 Overflow logs.

For generating reports and full inspection of each Event Log, each Event Log must be opened and manipulated from within the target Relational Database Software Product, providing the user unlimited report generation capabilities. This allows Event Log inspection and report generation via a user preferred Database Management System.

8.2 ALARM EVENTS

Alarm Events are defined as the transition of a data point from an Ok/Non-Faulted state to a Faulted state and vise versa. These Events are date and time stamped and contain information including the source of the event and a description of the Event.

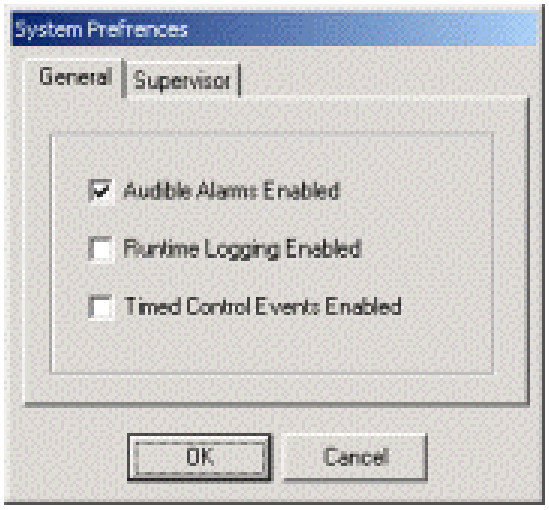
8.3 CONTROL EVENTS

Control Events are defined as any attempted user initiated system device control command. These Events are date and time stamped and contain information including the User Name who was logged into the system at the time the attempted command with initiated, the target device of the command, a description of the command, and the value of the attempted command. It is important that the user understand that a control event only tracks ATTEMPTED control events and does not guarantee that the Control Event was successfully implemented by the target device in question.

8.4 RUNTIME DATA EVENTS

Runtime Data Events are user defined. The Runtime Data Event Logging mechanism allows the user to log the value of any number of device data points to the Runtime Data Event Log, based on a user selectable Delta Trigger Value or time interval. The Runtime Data Event Logging can be enabled or disabled on a global level, like a master on off switch, and individually for every point of every device in the system (with some exceptions in some systems). When the Global control is disabled, via the Preferences submenu of the Main Window System menu (See Figure 8.1), no runtime data logging will take place. When the Global control is Enabled, runtime data logging will take place only for device data points that have been individually enabled for runtime data logging via the Device Logging Info window accessible from each device screen.

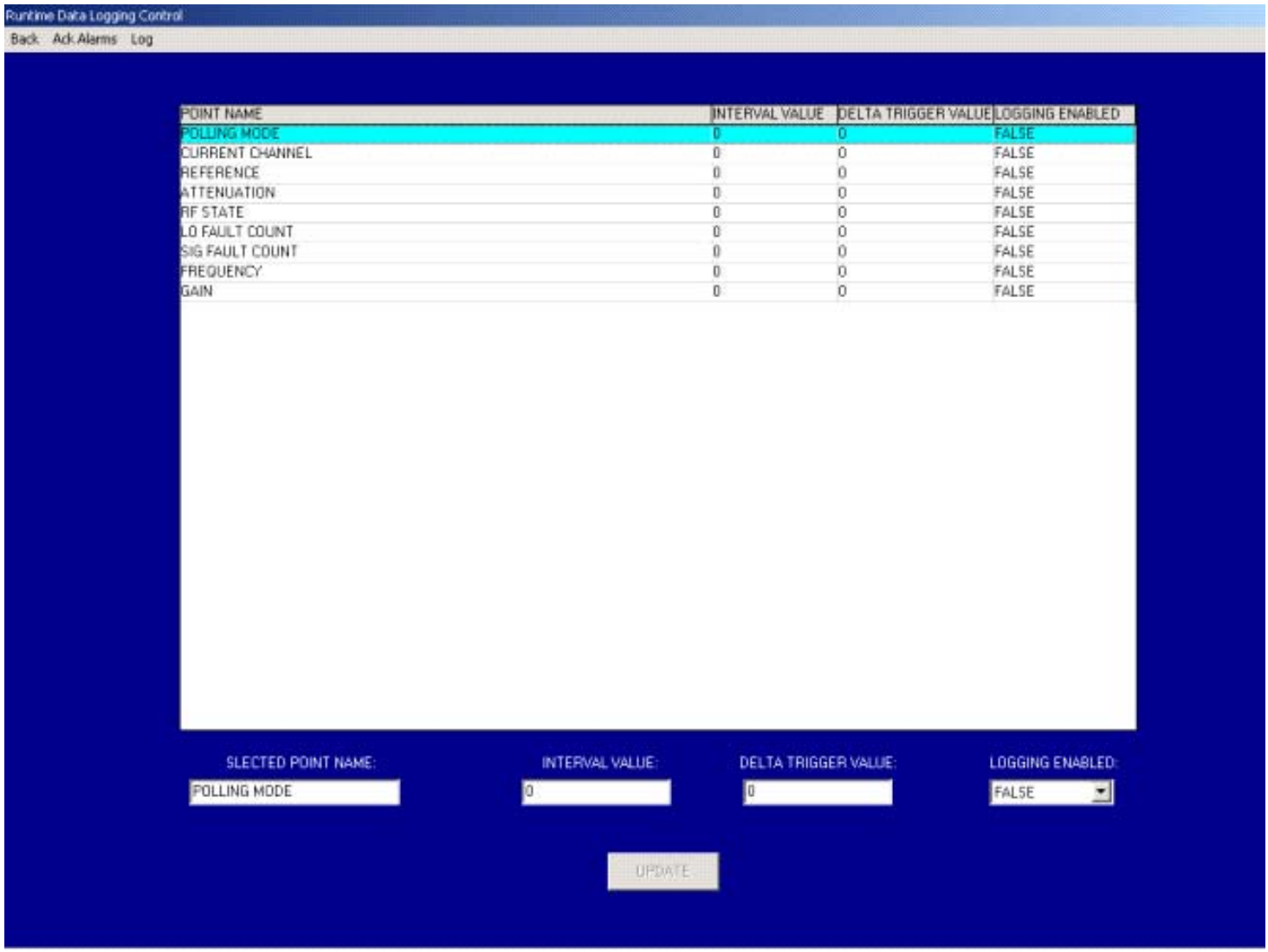
Figure 8.1 System Preferences Selection Dialog



The Runtime Data Event Logging mechanism is based on a user selectable Delta Trigger Value or time interval which is controlled via the Runtime Data logging Control Window accessible from the “Configure” Menu item in each Device Window (See Figure 8.2). For points with a delta trigger value defined, every time the data point changes values, the new value is compared with the last logged value. If the difference, or Delta, between these two values is larger than the user editable Delta Trigger Value for the point, then a Runtime Data Event is logged. Each Event contains the Date and Time stamp for when the event was logged, the subsystem, device, and

point name of source of the event, and the value of the point. For points with an interval value, the value will be logged periodically on the interval value.

Figure 8.2 Runtime Data logging Control Window



To enable a point for logging:

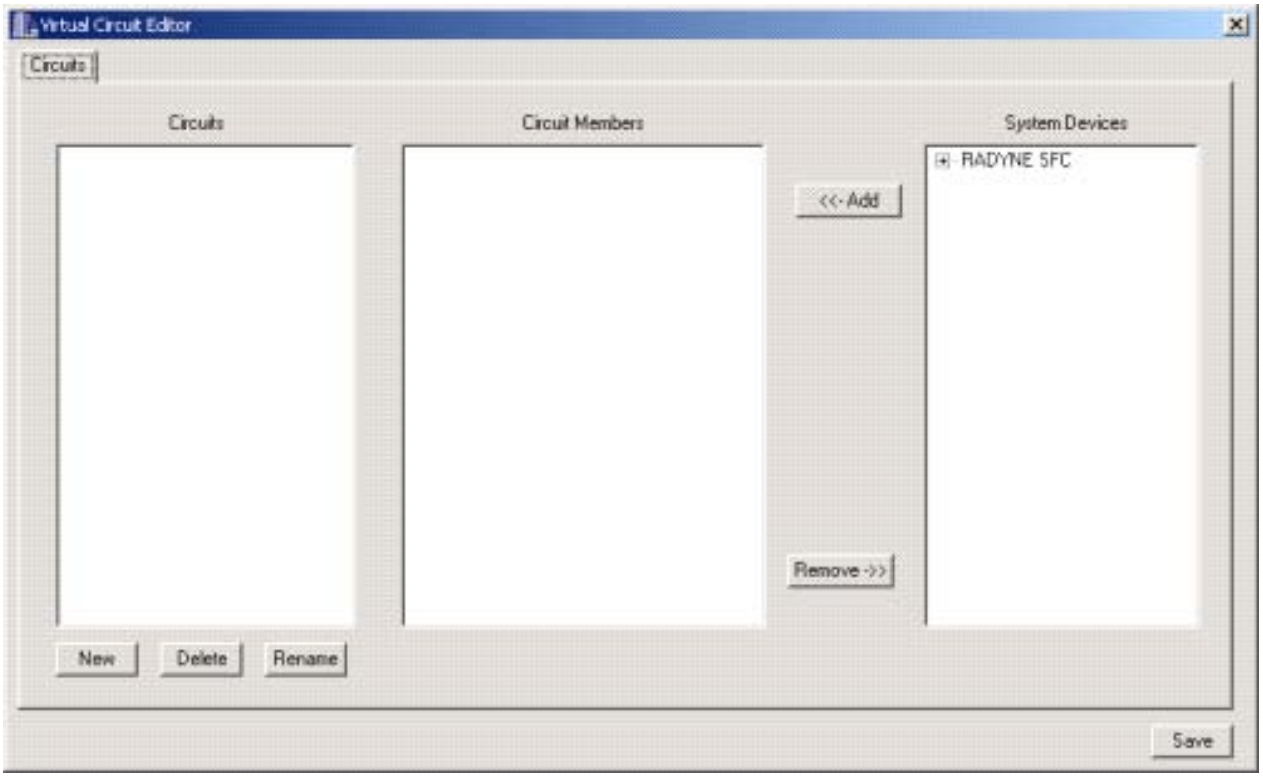
1) Select the desired point from the list
2) Enter either a desired interval value (in Min) or Delta trigger value in the respective field
3) Select TRUE from the Logging Enabled Field
4) Select the Update Button

Note: For state type points such as ON/OFF values, use a Delta Trigger Value of 1 to log state changes.

9.0 VIRTUAL CIRCUITS

VisiNet provides the user a mechanism to logically associate the Status of any number of individual devices to a user defined element called a Virtual Circuit. The Virtual Circuit represents the Logical OR-ing of the status of all its member devices. The Virtual Circuits are treated as Fault Status Points by the system and in turn are process by the Alarm Event Reporting Subsystem. This allows users to create Virtual Circuits that report a single Fault status point that represents the accumulated status for multiple devices. Virtual Circuits are created and edited using the Virtual Circuit Editor accessible from the "Supervisor" Menu item of the Main Window (See Figure 9.1).

Figure 9.1 Virtual Circuits Editor Window



Window Elements

Element	Description
Circuits List	List all existing circuits
Circuit Members List	List all member devices for the selected circuit
System Devices List	Lists all Devices in the system
New Button	Creates a New circuit
Delete Button	Deletes the selected circuit
Rename Button	Renames the selected circuit

Add Button	Adds the selected device to the selected circuit
Remove Button	Removes the selected device from the selected circuit

To create a Virtual Circuit:

1) Select the New Button
2) Select a device from the System Devices List
3) Select the Add button
4) Repeat steps 2 and 3 as desired
5) Select the Save button when complete.

10.0 MAINTAINANCE AND TROUBLESHOOTING

VisiNet is designed to be virtually maintenance free. The only maintenance required to be performed by the system administrator is the backup of the overflow Event Log files located in the Runtime directory. As discussed in Section 7 on Event reporting, if these files are not backed-up, they will be deleted once they all become full.

Should the NMS start to perform erratically, check all cabling, device addresses, device communication parameters. If problems persist, shut down the NMS and check the contents of the driver debug files located in the Visinet/Drivers/particular device's driver directory for driver error messages. If there are any entries in the device debug files, save a copy of the file in a different directory for inspection by IST Personal. Try restarting the NMS. If the problems still persist, contact IST for further instructions.

Device Driver can be used in a special mode to assist in debugging communication problems. This mode is a loop-back mode where the driver will send a series of test message out the communications port, wait for the exact message to be received on the same port, and report the result to the user. Running the Driver in this loop-back mode can be used the validate the communications path from the NMS computer, through the communications cables, to the end device. To use the driver loop-back mode to debug communications problems, start by shutting down the NMS and make sure that all the device drivers have also shutdown. Then shut down the FEP server by selecting the FEP.exe process in the "Processes" tab from within the Microsoft Windows Task Manager and selecting "End Process". This is the KEY to running the driver in the loop-back mode. When a Driver starts up, it first looks for the FEP server process and if the FEP is running it continues normal startup operations. If the FEP is not running, it asks the user if they want to run a loop-back test. Enter "Y" for yes or "N" for no. The driver will continue in the mode until the user select "N" at which point the driver will shut down. If "Y" is selected, the loop-back test will run 10 times and display the results of each test then prompt the user to continue.

Once the system is ready to run the loop-back test, create a loop-back connection on the end of the communications cable that connects the computer to the device in question by connecting the connectors Transmit pin(s) to the Receive pin(s). The actual pins in question will depend on the device in question so refer to the user's manual for the device. If you are uncertain of this process please contact the NMS or Device manufacture for assistance because improper connections can permanently damage the HW in the system.

APPENDIX A: SYSTEM INSTALLATION

INSTALLATION INSTRUCTIONS

To properly install the NMS, the following instructions MUST be performed by a user logged into the target computer as the NT Administrator or a user that has been assigned Administrator privileges.

INSTALLATION CD ROM

The NMS comes with an installation CD ROM that contains all the necessary files for the installation.

INSTALLATION TYPE

The NMS can operate in two modes, Master/Sever and Client, and the installation for each type varies slightly. The Server mode comprises the entire NMS and must be installed on the Master (Server) computer system. This is the computer system that will be connected to all the equipment to be interfaced to. For Stand alone single user systems, this is the type of system that must be used. The Client mode comprises just the GUI (Graphical User Interface) and is used to connect to the Server from a remote computer connected to the Master computer via a TCP/IP network.

INSTALLATION OVERVIEW

The NMS installation is a Three (3) step process. The First step Prepares the computer for the NMS Installation. The Second step installs all the required files for the VisiNet NMS. The Third step depends on the type of installation performed. For Master type of install, the third step installs the required drivers for the License Control System (LCS). For Client type of install, the third step involves setting up information required to connect to the remote Master NMS Server.

1 - PRE-INSTALLATION

1)
Log into the Microsoft OS as Administrator or a user that has been assigned Administrator Privileges.

2)
Shutdown any applications that may be currently running on the computer.

3)
If re-installing, or installing a newer version of VisiNet onto a computer already loaded with the VisiNet NMS, rename the existing VisiNet folder located on the computer's C drive to some other name like "OLD Visinet". This is required to ensure that all the files of the New installation are guaranteed to be installed properly, while also allowing the user to revert back to the previous version should problems arise with the newer version.

4)

Connect the HW KEY delivered with the installation media to either the master NMS computer's parallel or USB port depending on the type of Key delivered.

2 - VISINET INSTALLATION

Insert the installation CD ROM into the computers CD ROM. Select the "Control Panel" option from the "Settings" option from the "Start" option from the task bar at the bottom of the Screen. Double click via the mouse the "Add/Remove Programs" Icon . Next Select the "Install" option from the Add/Remove Programs dialog box. Select the "Next" Option. Select the "Browse" button and navigate to the "Setup.exe" file located in the "Install" on the CD ROM. Once this file is visible in the command line, select the "Finish" option to initiate the NMS installation. The first dialog box will ask the user to make sure all applications are closed. If all applications are closed select the "Next" option to continue, else select the "Cancel" Option to abort the installation and close all open applications and restart the installation. Once past this point, the user will be prompted to select the type of installation desired. Select the desired type depending on the following:

Typical
This type installs the entire (Master) NMS (GUI client, FEP Server, and all device drivers) and must be installed on the Master (Server) computer system. This is the computer system that will be connected to all the equipment to be interfaced to.

Compact
This type is the same as "Typical" without the Documentation.

Custom
This type allows the user to install either the entire (Master) NMS as in the "Typical" installation type, or a Client mode NMS that comprises just the VisiNet GUI (Graphical User Interface) and related support files required to connect the GUI client to a Remote Master NMS Server. Select this type to install a VisiNet GUI for Remote NMS Capabilities via a TCP/IP network connection to the NMS Master Computer.

At the bottom of this window, the user is presented with the "Destination Directory" that **MUST** be "C:/Visinet/Gui". If the default directory does not indicate C:/Visinet/Gui, select the "Browse" button to change the installation directory to "C:/Visinet/Gui".

To complete the installation select the "Next" button and follow the instructions presented by the installation setup program. Once the installation has been verified, the old Visinet folder, if one was created in step 1 can be deleted safely.

3 – LCS INSTALLATION (FOR MASTER TYPE OF INSTALLATION)

If performing an entire Master (Server) NMS Installation, install the License Control System (LCS) Drivers by running the "hdd32.exe" located in the VisiNet directory and follow the directions provided by the installation utility. Wait Until you have been prompted that the installation is complete. This may take a few minutes so please be patient.

3 – SERVER INFO SETUP (FOR CLIENT TYPE OF INSTALLATION)

If performing a Client type NMS Installation, open the "NMS.cfg" file located in the "C:\Visinet\Gui\System" directory with a text editor and change the second element of the second line to the IP address of the Master Computer running the FEP to connect to. This element will currently be set to the standard IP Loop back address of 127.0.0.1.