

**INTEGRATED SOFTWARE TECHNOLOGIES INC.**

**VisiNet™**

**Network Management System**

**A Technical Description**

# TABLE OF CONTENTS

<b>1.0 INTRODUCTION</b> .....	<b>3</b>
<b>2.0 VISINET OVERVIEW</b> .....	<b>4</b>
2.1 INTRODUCTION.....	4
2.2 DEFFINITION:.....	4
2.3 FEATURES:.....	4
<b>3.0 VISINET DEFFINITION</b> .....	<b>5</b>
3.1 INTRODUCTION:.....	5
3.2 ARCHITECTURE: .....	5
3.2.1 <i>GUI ARCHITECTURE</i> : .....	7
3.3 USER INTERFACE:.....	8
3.4 FEATURE SET:.....	10
3.4.1 <i>ALARM INDICATIONS</i> : .....	11
3.4.2 <i>SECURITY</i> : .....	12
3.4.3 <i>EVENT REPORTING</i> :.....	12
3.5 INSTALLATION AND MAINTAINANCE: .....	12
<b>4.0 WARRANTY AND LICENSE</b> .....	<b>13</b>
4.1 CUSTOMER SATISFACTION:.....	13
4.2 LICENSE: .....	13
4.3 WARRANTY:.....	13

## 1.0 INTRODUCTION

---

Since 1996, Integrated Software Technologies has been providing the Satellite Communications Community with products to handle all of their Network Management requirements. With systems in operations throughout the globe, IST has proven itself as a world class supplier of reliable, cost effective Network Management products. Along with quality products, IST is committed to providing all of its customers with TCS (Total Customer Satisfaction) through unparalleled Customer Service and Support.

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 Windows 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).

We at IST take great pride in our products and services and will continuously work at providing our customers with the highest quality products and services available, while also striving to improve the customer's overall buying experience.

## **2.0 VISINET OVERVIEW**

---

### **2.1 INTRODUCTION**

This section provides a high level description of Integrated Software Technologies Inc., IST's, Network Management System (NMS) product/framework VisiNet™, including an overview of the standard features of the product.

### **2.2 DEFFINITION:**

Integrated Software Technologies Inc., IST's, Network Management System (NMS) product/framework VisiNet™, is a PC based Network Management System 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 native Microsoft Windows NT workstation 4.0/ Win2K application making it easily installed, operated, and maintained. The distributed nature of the system's architecture 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.

### **2.3 FEATURES:**

VisiNet™ provides the user with a robust set FCAPS of features similar to those found in Network Management Products offered by other vendors. 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. Further feature descriptions and definitions will be presented in subsequent sections of this document.

- 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

## 3.0 VISINET DEFFINITION

---

### **3.1 INTRODUCTION:**

This section provides a detailed description of the Standard VisiNet™ product including System Architecture, User Interface, Feature set, Installation and Maintenance issues.

### **3.2 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

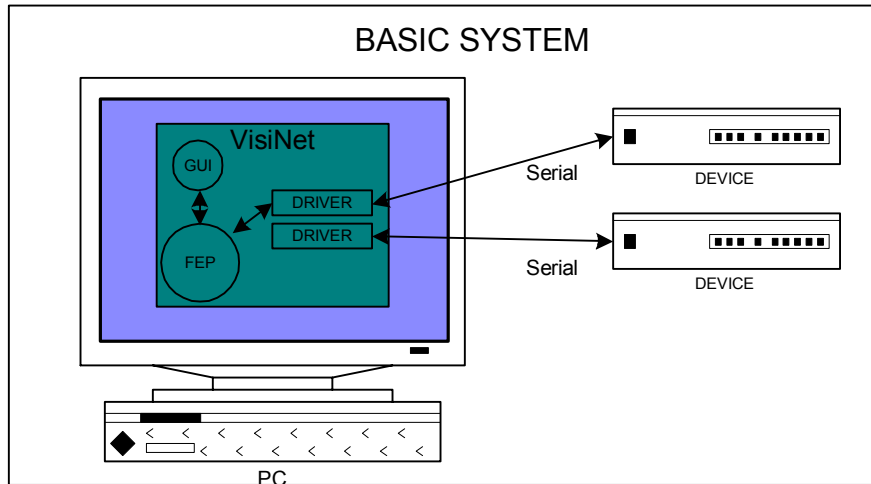
The Graphical User Interface (GUI) is the portion of the system that the user(s) visually see and interact with. It comprises all the user interface features and capabilities such as device management, fault management, security management, fault management, and event reporting. As far as the general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

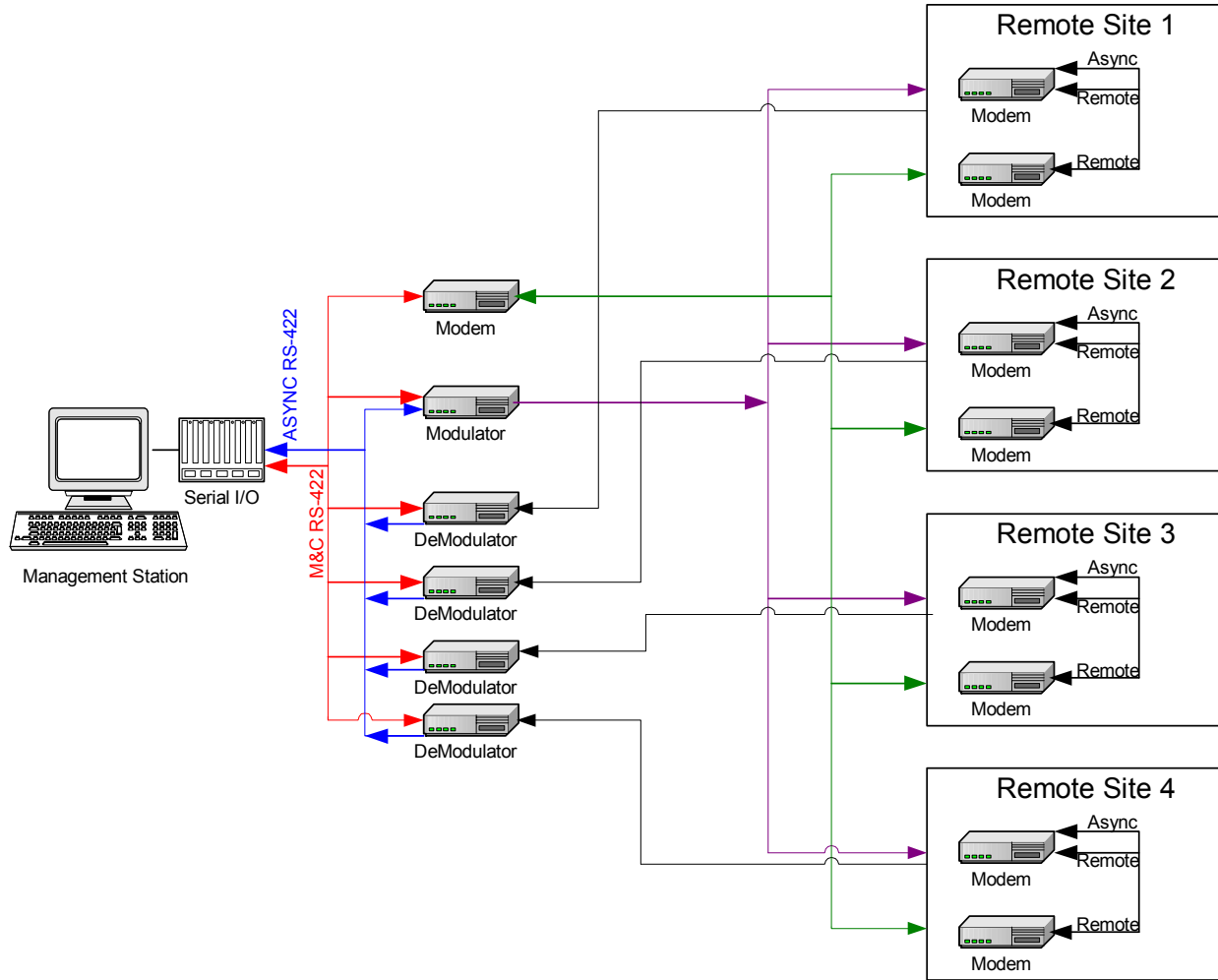
See Figure 3.1 for a general system architecture diagram.

Figure 3.1 Basic System



The distributed capabilities of the system are achieved by 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 3.2 provides a sample system diagram for a basic VSAT type of application.

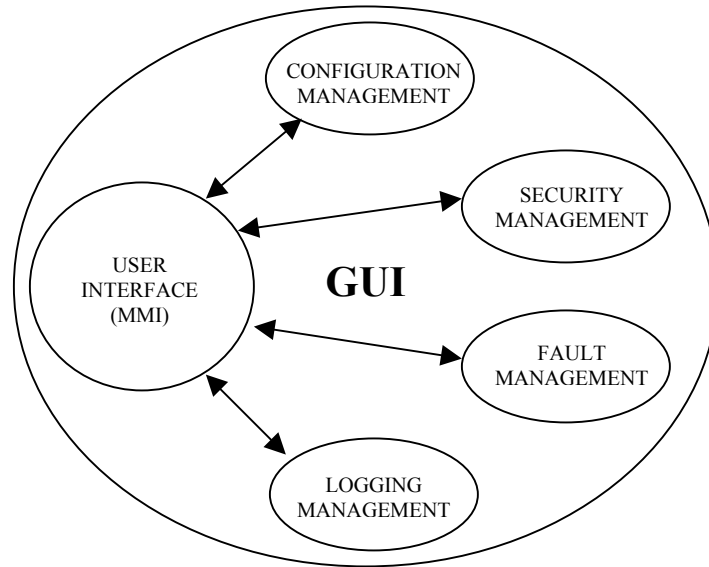
**Figure 3.2 Sample VSAT Application**



### **3.2.1 GUI ARCHITECTURE:**

As mentioned above, the GUI is the portion of the system that the user(s) visually see and interact with. It contains and implements all the user interface features of the NMS autonomously and independent from any other GUI clients that may be present in the overall system. This means that for systems where multiple GUI clients exist, each GUI client operates off of, and maintains its own local implementations of, such user interface features as device management, fault management, security management, and event reporting. The GUI is functionally comprised of many different elements, with each element providing and implementing a logical group related features/services to the User. This structure of different elements can be seen in the basic architecture diagram of the GUI, Figure 3.3

**Figure 3.3 GUI Architecture**



- A. The User interface, termed Man Machine Interface (MMI), element handles all user interaction and user interface generation such as system and device views.
- B. The Configuration Management element handles all GUI configuration issues such as Supervisor related system options/preferences.
- C. The Security Management element handles all the security issues such as user account creation, configuration and user log-in/log-out operations.
- D. The Fault Management element handles all the Fault related issues such as fault generation, correlation, filtering, and action.
- E. The Logging Management element handles all the event logging related issues for the different event logging features provided such as Alarm Event logging, Control Event logging, and Runtime Data Event logging.

### **3.3 USER INTERFACE:**

The system's user interface, termed Man Machine Interface (MMI) or Graphical User Interface (GUI), 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 drawings and diagrams while utilizing colors to present the status of these different elements. Standard color coding is as follows:

- RED indicates a major alarm condition
- YELLOW indicates a Minor alarm/warning condition
- ORANGE indicates a Maintenance mode condition
- PURPLE indicates an Invalid Data condition

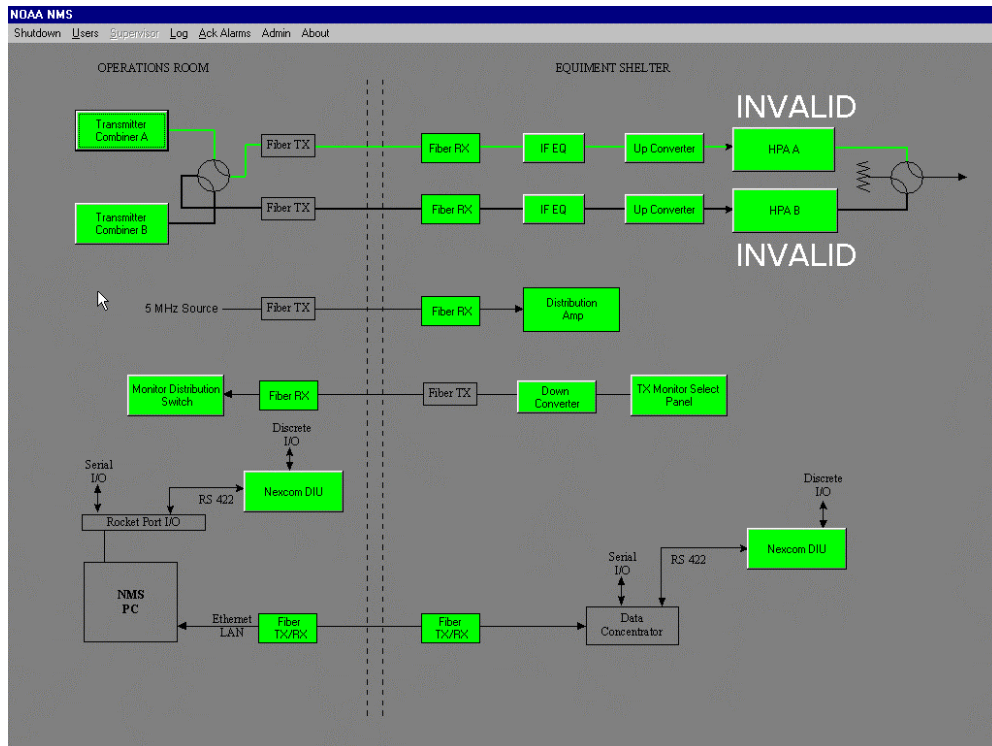


- GREEN indicates an OK condition.

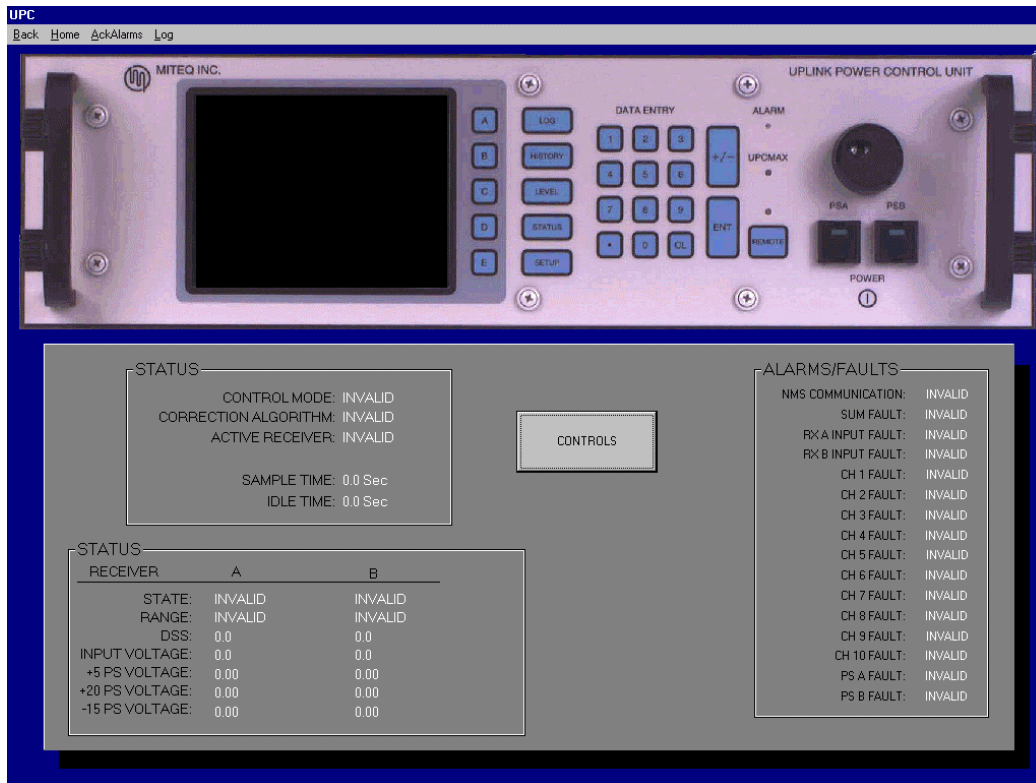
The presence of an unacknowledged event is represented by active object blinking. This system of objects, colors, and blinking provides for a very intuitive interface, regardless of the complexity of the system being monitored.

All customer equipment under management is represented in the NMS by graphical objects. These objects are precise drawings of the equipment's front panel. In some cases, actual front panel indications such as status LED's are present on the graphical object and react in real-time to the device. This unparalleled high level of graphics provides the user with a very comfortable and non-intimidating operating environment. The following figures present examples of a Main Screen and a Device Screen from past systems. To view more sample screens from past systems, please visit [www.istisw.com](http://www.istisw.com) and follow the links to the Sample Screens section.

### Sample Main Screen



## Sample Device Screen



Since each system is different, and each customer's requirement unique, IST works hand in hand with the customer during the design phase to produce a system wide user interface that best meets the customer's desires.

### 3.4 FEATURE SET:

VisiNet™ provides the user with a robust set of features similar to those found in other FCAPS types Network Management Products offered by other vendors. 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 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.

### **3.4.1 ALARM INDICATIONS:**

All system alarm set and clear events result in visual, and user configurable, audible indications presented to the user.

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.

### **3.4.2 SECURITY:**

VisiNet provides 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 Database. 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.

### **3.4.3 EVENT REPORTING:**

VisiNet provides three types of event reporting capabilities, Alarm, Controls, and Runtime data. All three data log event types are Date and Time stamped and stored in separate ODBC SQL relational databases. From within the NMS, the last 100 most recent events from each data log can be viewed in separate 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.

The Alarm data log contains all system Alarm set and clear events.

The Controls data log contains all user initiated device control events with each event containing information on which user initiated the event, the device, data point and new value of the initiated control event.

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 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.

## **3.5 INSTALLATION AND MAINTAINANCE:**

VisiNet is designed to be easy to install, should the need arise, and virtually maintenance free. The NMS is delivered turnkey, with a set of installation media should the system need to be reinstalled. This installation procedure is a two-step process that can be successfully performed by a junior level technician with basic Microsoft Windows skills. A full installation of each instance of VisiNet can be typically completed within a matter of minutes. The Visinet installation media is delivered as a standard Microsoft installation media with explicit instructions on the installation procedure in the form of a text file. The only maintenance required is the periodic archiving of event log files and the management of user accounts.

## **4.0 WARRANTY AND LICENSE**

---

### **4.1 CUSTOMER SATISFACTION:**

All IST Network Management Systems are designed from the start with customer satisfaction being priority 1. This is accomplished by involving the customer in all phases of the design process. The customer is especially encouraged to participate in the design of the system's screens that make up the user interface. This close working relationship with the customer ensures the delivery of a Turn Key Network Management System that meets or exceeds all customer expectations.

### **4.2 LICENSE:**

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 in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

### **4.3 WARRANTY:**

IST warrants its VisiNet NMS product against internal software defects for a period of one year after the date of installation of the system, or one year and three months after the date of official purchase of the product, whichever is shorter. Extended Warranty can be purchased in 1-year increments. Software defects are defined as programming bugs that are present in the VisiNet product and do not include system upgrades, changes requested for aesthetic or operational modifications, or problems related to defects in external elements such as operating systems and devices being managed.