Network Manager

Application Note # 01

March 8, 2021
00DA0109-001, Rev X

Network Manager overview

Network Managers

The Network Managers (NM) handle the alarm data management for Senstar's proprietary security networks. The Network Manager is available either as a Windows Application on the Network Manager CD (kit # 00FG0200) or as a Windows Service on the Network Manager Suite CD (kit # 00FG0220). There are three variants of the NM Application, one each for the Sentrax, Voice over Ethernet (VoE), and MX networks. The Network Manager Service handles the alarm data management for the Silver, FiberPatrol, CCC, Crossfire, Krypton, Sennet, and Starcom networks.

The NM Applications and the NM Services function as data servers which collect and distribute alarm point data and control point status for third party Security Management Systems (SMS) via the Network Manager Interface (NMI) or generic text, or legacy Starcom protocol (Contact Senstar Customer Service for Starcom protocol details). The third party organization is responsible for writing the software, which establishes communication to the Network Manager and implements the NMI.

Software developers have 2 choices when implementing the NMI:

- establish the TCP/IP communication and process raw NMI messages;

OR

- use an MFC DLL, which provides a higher level integration to the NMI TCP/IP messages.

Both methods are supported by the Network Manager software, to provide developers greater flexibility when interfacing to the NM products. The Network Manager Interface Software Development Kit (SDK) includes the files necessary for developing an interface. It also demonstrates the two methods through sample programs, written in C++ for Windows MFC framework. The programs serve as examples and test applications, and all source code is included.

If a developer is using raw NMI messages and redundant Network Managers, the application can connect to only the active NM. Therefore, when trying to connect to redundant Network Managers initially, or after losing the connection, you must hunt between the two specified IP addresses for the active NM.

Lenel OnGuard

The Network Manager Service supports integration to the Lenel OnGuard 2010, 2012, 2013 and 7 security management systems.

Note For implementation details, refer to application note 00DA0309 - Network Manager Service/OnGuard Integration.

Genetec Security Center

The Network Manager Service supports integration to the Genetec Security Center (GSC) security management system with the addition of the Genetec-Senstar Gateway (Senstar p/n 00SW0260).

Note	Requires the addition of a Senstar NMS SDK license (Genetec p/n GSC-1SDK-SENSTAR-NMS) to the Genetec Security Center.

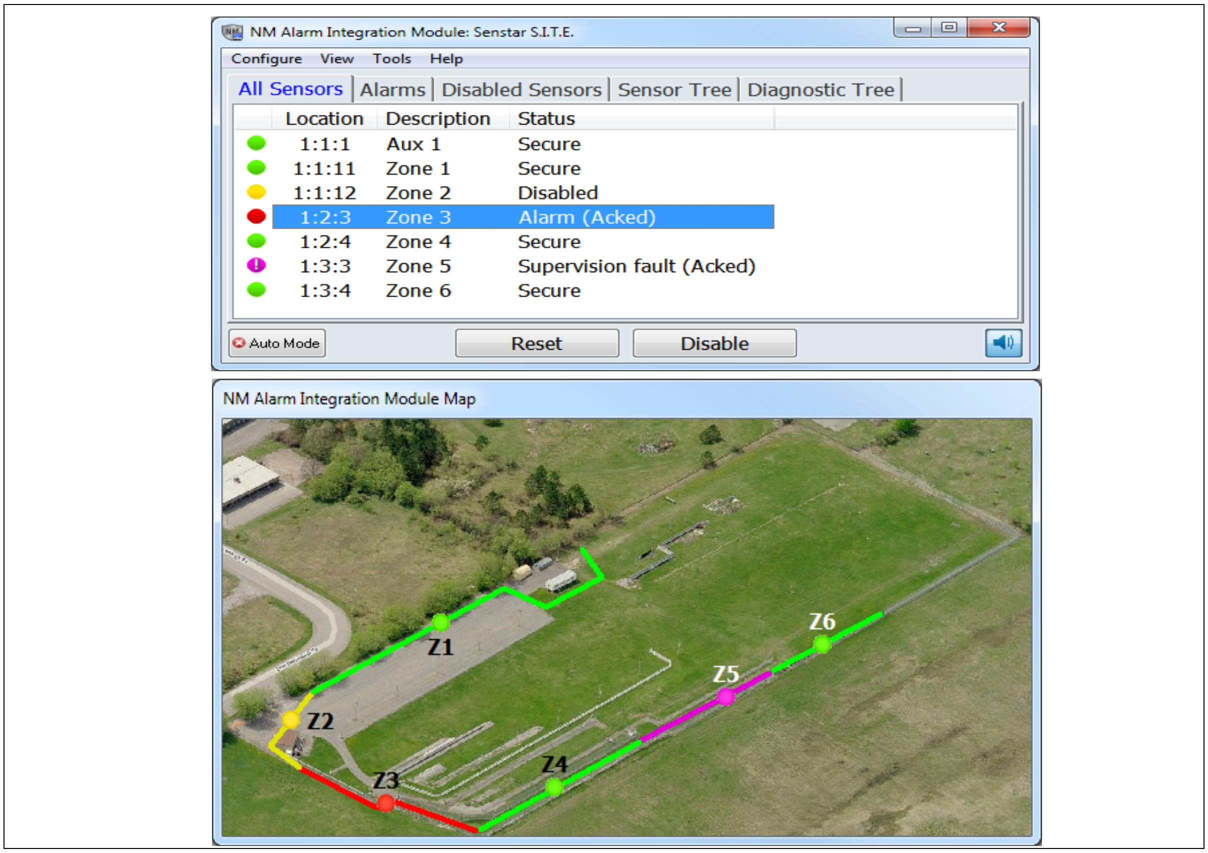
Note	For implementation details, refer to application note 00DA0409 - Network Manager Service/Genetec Security Center Integration.

Network Manager Alarm Integration Module

The Network Manager Alarm Integration Module is a text-based Security Management System that can display the alarm status for up to five Network Managers. Optionally, a status map can be configured to graphically display the status of the sensor alarms.

The Alarm Integration Module can run on the same computer as the Network Manager(s), or it can run on any computer that has a network connection to the NM computer. Communication to the NMs is through the Network Manager's SMS connections. A hardware license dongle is required to run the Alarm Integration Module. Without the dongle, the Alarm Integration Module will run in demonstration mode for a period, and then shut down.

Figure 1: illustrates the Alarm Integration Module textual display (All Sensors tab) along with a graphical map display of the same site conditions.


NM Alarm Integration Module: Senstar S.I.T.E.
Configure View Tools Help
All Sensors | Alarms | Disabled Sensors | Sensor Tree | Diagnostic Tree
Auto Mode
Reset
Disable
NM Alarm Integration Module Map
Z1
Z2
Z3
Z4
Z5
Z6

	Location	Description	Status
🟢	1:1:1	Aux 1	Secure
🟢	1:1:11	Zone 1	Secure
🟡	1:1:12	Zone 2	Disabled
🔴	1:2:3	Zone 3	Alarm (Acked)
🟢	1:2:4	Zone 4	Secure
❗	1:3:3	Zone 5	Supervision fault (Acked)
🟢	1:3:4	Zone 6	Secure

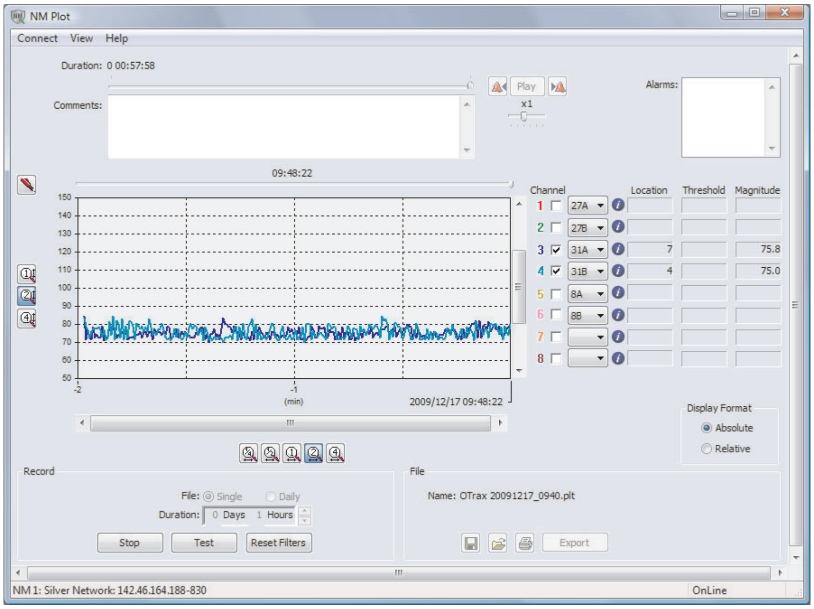
Figure 1: Example Alarm Integration Module textual and graphical map displays

Sensor Management Tools

Both the Network Manager CD and the Network Manager Suite CD include three tools which enable users to perform network wide sensor response plots, and collect NM Event Logs and Node Status information from remote locations without interrupting operations (see the SM tools' online help for details on using the tools). A fourth tool, the NMS Audio Tool (00SW0250) is available as an add-on to the Network Manager Suite. The NMS Audio Tool enables the user to listen to a digital representation of the audio signals from FlexZone sensor zones.

Plot tool

The Plot tool (NM Plot.exe) uses a Universal Configuration Module (UCM) TCP/IP connection to perform a network wide response plot for the selected sensor type. Supported sensor types include Silver Network-based OmniTrax processors, XField processors, FlexPS processors, FlexZone processors and UltraWave receivers; Crossfire-based Intelli-FLEX processors; Sennet-based Perimitrax Sensor Modules and Intelli-FLEX processors; and Sentrax Transceiver Modules (see Figure 2:).



Duration: 0 00:57:58

Channel			Location	Threshold	Magnitude
1	☐	27A			
2	☐	27B			
3	☑	31A	7		75.8
4	☑	31B	4		75.0
5	☐	8A			
6	☐	8B			
7	☐				
8	☐				

Display Format
● Absolute
○ Relative

File: ● Single ○ Daily
Duration: 0 Days 1 Hours

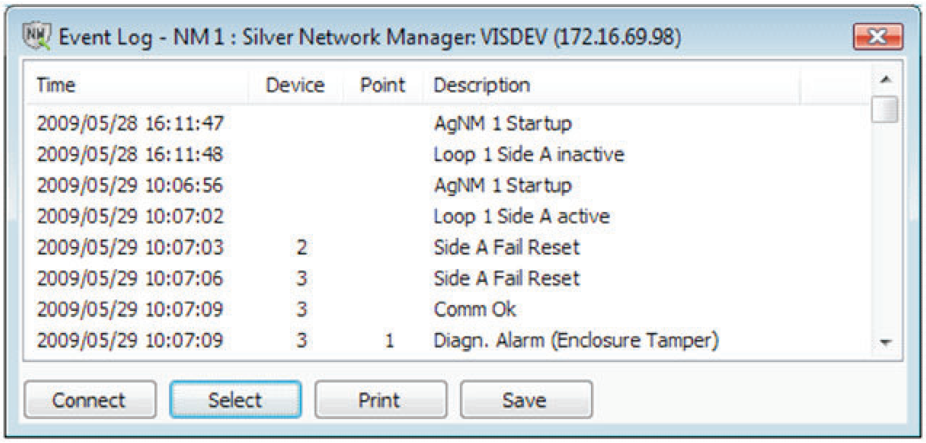
Name: OTrax 20091217_0940.plt

NM 1: Silver Network: 142.46.164.188-830 OnLine

Figure 2: Example NM Plot tool screen

Event Log tool

The Event Log tool (NM Event Log.exe) uses a UDP/IP connection to retrieve and display a NM's event log (see Figure 3:).



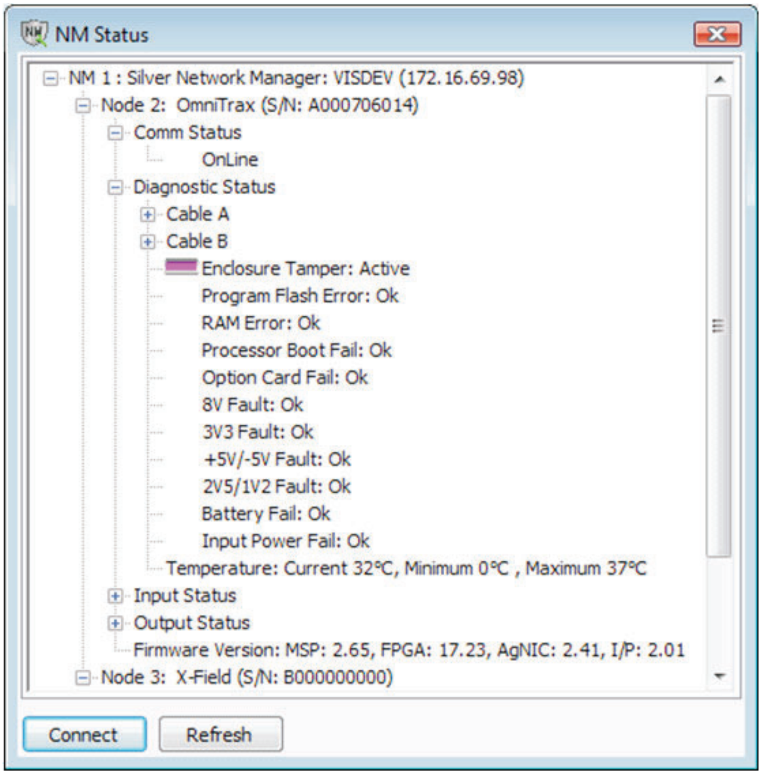
Event Log - NM 1 : Silver Network Manager: VISDEV (172.16.69.98)

Time	Device	Point	Description
2009/05/28 16:11:47			AgNM 1 Startup
2009/05/28 16:11:48			Loop 1 Side A inactive
2009/05/29 10:06:56			AgNM 1 Startup
2009/05/29 10:07:02			Loop 1 Side A active
2009/05/29 10:07:03	2		Side A Fail Reset
2009/05/29 10:07:06	3		Side A Fail Reset
2009/05/29 10:07:09	3		Comm Ok
2009/05/29 10:07:09	3	1	Diagn. Alarm (Enclosure Tamper)

Figure 3: Example NM Event Log tool screen

Network Manager Status tool

The NM Status tool (NM Status.exe) uses a UDP/IP connection to retrieve and display the status of a NM's nodes (network devices). The status of the nodes is displayed in a tree structure (see Figure 4:).



NM Status

```
⊟ NM 1 : Silver Network Manager: VISDEV (172.16.69.98)
   ⊟ Node 2: OmniTrax (S/N: A000706014)
      ⊟ Comm Status
            OnLine
      ⊟ Diagnostic Status
         ⊞ Cable A
         ⊞ Cable B
            🟪 Enclosure Tamper: Active
            Program Flash Error: Ok
            RAM Error: Ok
            Processor Boot Fail: Ok
            Option Card Fail: Ok
            8V Fault: Ok
            3V3 Fault: Ok
            +5V/-5V Fault: Ok
            2V5/1V2 Fault: Ok
            Battery Fail: Ok
            Input Power Fail: Ok
         Temperature: Current 32°C, Minimum 0°C , Maximum 37°C
      ⊞ Input Status
      ⊞ Output Status
      Firmware Version: MSP: 2.65, FPGA: 17.23, AgNIC: 2.41, I/P: 2.01
   ⊟ Node 3: X-Field (S/N: B000000000)
```

Figure 4: Example NM Node Status tool screen

NMS Audio tool (00SW0250)

The NMS Audio Tool (NMS Audio.exe) is a Windows application used to listen to a digital representation of the audio signals from FlexZone sensor zones via an Audio MUX node. The Audio MUX node is used to define the FlexZone sensor zones that require audio listen-in capability, and to define how those zones are presented. The Audio Tool can be used to listen to one zone, or to multiple zones, through the default audio device of the computer on which it runs. The Audio Tool can be run on any computer that has a network connection to the target NMS (see Figure 5:). The Audio Tool is available on CD as an add-on to the Network Manager Suite software.

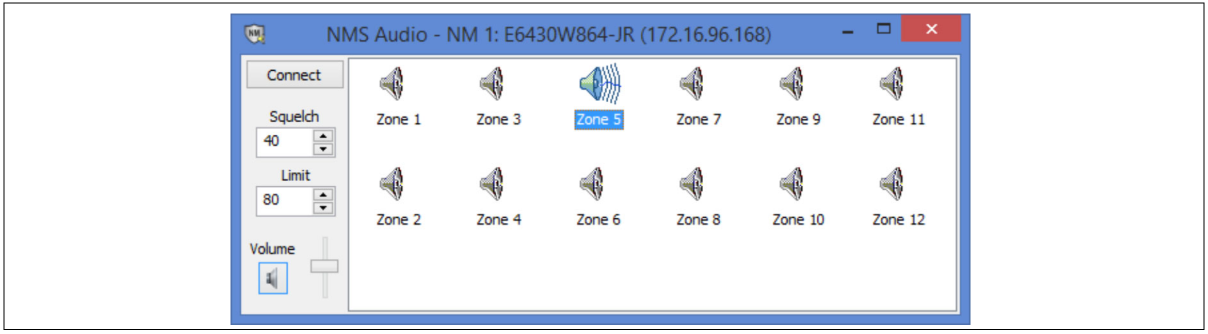


Figure 5: NMS Audio tool screen

Network Manager Simulator

The Network Manager Simulator (NMSimul) is used in place of a Network Manager to simulate the operation of a Network Manager with a connected network of security devices. Use NMSimul to test system databases before installing and connecting the network devices. Developers can also use NMSimul to test and verify the interfaces to third party Security Management Systems.

- The Network Manager Simulator can be configured to simulate Sentrax, VoE and MX Network Managers.
- Up to ten instances of the NMSimul can run on one PC.
- The NMSimul supports connections to one or two SMS's.
- The NMSimul can be configured for redundant operation on one computer by using separate working folders, or on two computers.
- As a security precaution, NMSimul breaks all connections to Security Management Systems once per hour. After a five second delay, NMSimul allows the connections to be re-established.

Note Refer to the online help for details about using the Network Manager Simulator.

Network Manager Service Simulator

The Network Manager Service Simulator (NMS Simul) is used in place of a Network Manager Service to simulate the operation of a Network Manager Service with a connected network of security devices. Use NMS Simul to test system databases before installing and connecting the network devices. Developers can also use NMS Simul to test and verify the interfaces to third party Security Management Systems.

- The Network Manager Service Simulator can be configured to simulate Silver, FiberPatrol, CCC, Crossfire, Sennet and Starcom Network Managers.
- Up to ten instances of the NMS Simul can run on one PC.
- The NMS Simul supports connections to up to four SMS's via the NMI.
- The NMS Simul supports connection to a Lenel OnGuard Comm Server.
- The NMS Simul can be configured for redundant operation on one computer by using separate working folders, or on two computers.
- The NMS Simul supports a UCM connection for Silver Network based processors. The UCM is used for configuring additional cable zones for ranging sensors, beyond the default zones of Cable A = Zone 1 & 2 and Cable B = Zone 3 & 4.
- As a security precaution, NMS Simul breaks all connections to Security Management Systems once per hour. After a five second delay, NMS Simul allows the connections to be re-established.

Note	Refer to the online help for details about using the Network Manager Service Simulator.

Figure 6: is a block diagram illustrating the correct vs. incorrect usage of NMSimul and NMS Simul.

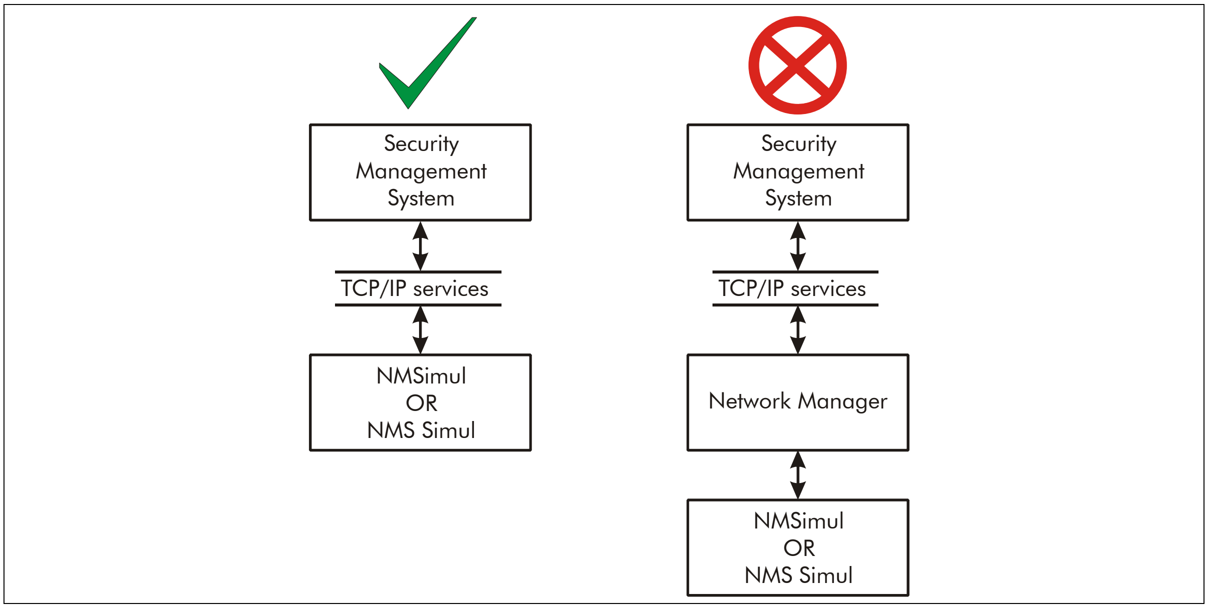


Figure 6: Correct vs. incorrect NMSimul and NMS Simul usage

Network Manager Interface

The Network Manager Interface is the message interface, which an SMS uses to communicate with a Network Manager. Using the NMI enables the SMS to collect alarm data and distribute control data for a Silver, FiberPatrol, CCC, Crossfire, Krypton, Sennet, Sentrax, Starcom, VoE, or MX network of intrusion detection sensors and security equipment. Communication with the security networks is via serial port or Ethernet. (The Silver Network can also use a USB connection via the NIU. FiberPatrol, Krypton and VoE communications are via Ethernet only).

The SMS can reside on the same computer as the Network Manager, or can communicate with an NM located on another computer. In both cases, TCP/IP is used. Network communication between computers is via Windows operating system services. Communication is carried out on a client-server basis, with alarm data changes sent unsolicited to the Security Management System (the client).

Alarm shunting

A common perimeter alarm processing concept is the ability to shunt (bypass/mask/access) alarms so that they are not reported to an operator. This feature is often used to prevent the reporting of alarms caused by normal traffic during the business day then re-enabling alarm reporting at night. Typically, there are two ways that Security Management Systems implement this feature.The SMS can either implement the alarm shunting internally and process raw alarm messages from sensors, or the SMS can request the sensor to shunt the alarms and then process alarms that are filtered by the state of the shunt.

The Network Manager supports both methods by sending separate messages to indicate the raw sensor alarm status, and the sensor alarm status that is filtered by the state of a shunt. Depending on how the SMS implements shunting, it then chooses which message type to processes (raw or filtered).

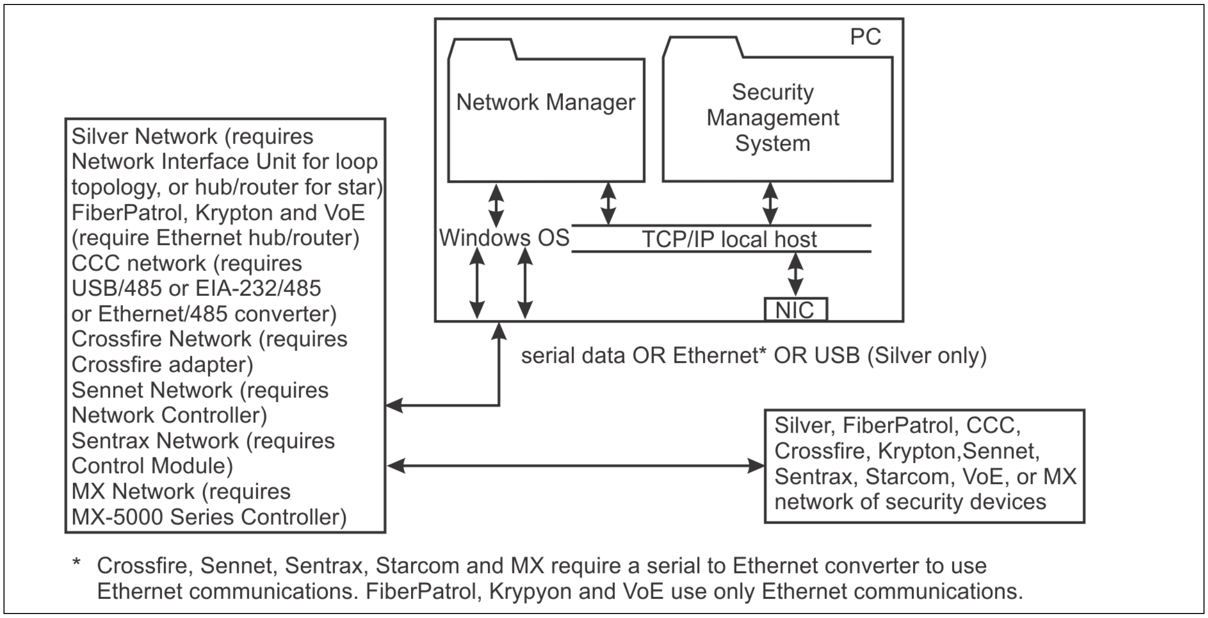
When an alarm occurs the Network Manager always sends a “raw sensor alarm” message to report the occurrence. If the shunt associated with the alarm is NOT set, then the Network Manager also sends a “filtered sensor alarm” message (i.e., if the shunt is set, then the filtered message is not sent). The design of the SMS determines which type of alarm messages (raw or filtered) it processes to obtain alarm information.

Communications

A Security Management Systems opens the TCP/IP socket for a Network Manager on a specific computer. The SMS then passes and receives messages from the Network Manager, as defined in the NMI. The NMI generally consists of short messages describing a status change for a particular alarm point. Bandwidth utilization is very low, typically consisting of alarm point traffic (a few IP packets).

Each Network Manager is responsible for the alarm data management for one sensor network (Silver, FiberPatrol, CCC, Crossfire, Krypton, Sennet, Sentrax, Starcom, VoE, or MX). Up to ten Network Managers can reside on a single computer, with each NM distinguished by a unique Unit ID. The NM Service and all variants of the NM Application can reside on one computer, enabling the connection of any combination of sensor networks, to a maximum of ten.

Figure 7: illustrates a Security Management System using the NMI to communicate with a Network Manager on a single PC. Both programs reside on the same computer, communicating over the TCP/IP local host. The Network Manager is responsible for the alarm data management for the Silver, FiberPatrol, CCC, Crossfire, Krypton, Sennet, Sentrax, Starcom, VoE, or MX network devices. The Security Management System serves as the operator interface to the security equipment.


PC
Network Manager
Security Management System
Windows OS
TCP/IP local host
NIC
Silver Network (requires Network Interface Unit for loop topology, or hub/router for star)
FiberPatrol, Krypton and VoE (require Ethernet hub/router)
CCC network (requires USB/485 or EIA-232/485 or Ethernet/485 converter)
Crossfire Network (requires Crossfire adapter)
Sennet Network (requires Network Controller)
Sentrax Network (requires Control Module)
MX Network (requires MX-5000 Series Controller)
serial data OR Ethernet* OR USB (Silver only)
Silver, FiberPatrol, CCC, Crossfire, Krypton,Sennet, Sentrax, Starcom, VoE, or MX network of security devices

* Crossfire, Sennet, Sentrax, Starcom and MX require a serial to Ethernet converter to use Ethernet communications. FiberPatrol, Krypyon and VoE use only Ethernet communications.

Figure 7: NMI on a single PC

Figure 8: illustrates a Security Management System using the NMI to communicate over a network with a second computer running the Network Manager. The NM computer is responsible for the alarm data management for the network devices. The SMS computer serves as the operator interface to the security equipment.

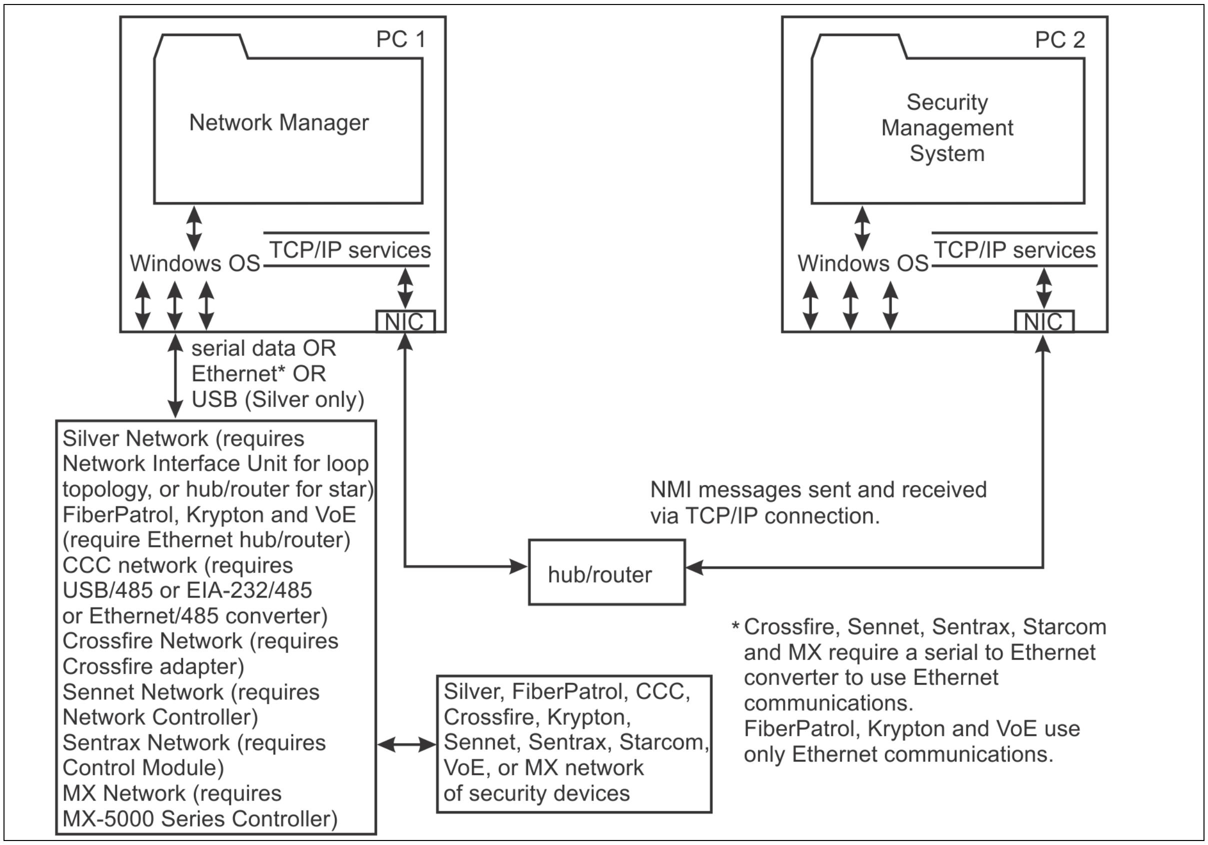

PC 1
Network Manager
Windows OS
TCP/IP services
NIC
serial data OR
Ethernet* OR
USB (Silver only)
Silver Network (requires Network Interface Unit for loop topology, or hub/router for star)
FiberPatrol, Krypton and VoE (require Ethernet hub/router)
CCC network (requires USB/485 or EIA-232/485 or Ethernet/485 converter)
Crossfire Network (requires Crossfire adapter)
Sennet Network (requires Network Controller)
Sentrax Network (requires Control Module)
MX Network (requires MX-5000 Series Controller)
hub/router
Silver, FiberPatrol, CCC, Crossfire, Krypton, Sennet, Sentrax, Starcom, VoE, or MX network of security devices
PC 2
Security Management System
Windows OS
TCP/IP services
NIC
NMI messages sent and received via TCP/IP connection.
* Crossfire, Sennet, Sentrax, Starcom and MX require a serial to Ethernet converter to use Ethernet communications.
FiberPatrol, Krypton and VoE use only Ethernet communications.

Figure 8: NMI via network communications

NMS hardware fail notification

In a basic unidirectional integration between the Network Manager Service (NMS) and a third party security management system (SMS) in which there is no audit of NMS status, an NMS crash, NMS PC failure, or a communication failure can go undetected. To protect against this, there is a hardware solution that will detect and report any Network Manager fail condition. The hardware solution uses an UltraLink I/O processor connected to a Silver Network Manager. The UltraLink processor includes a fault relay that is triggered by any NMS fail condition. This option will work even if the other sensors are on a different network. When multiple NMS are running on a PC, if one of them crashes, the Operating System causes the others to shutdown.

- The hardware solution uses an UltraLink I/O processor on a Silver Network to monitor the health of the NMS. The UltraLink's fault relay is activated by an NMS failure. The fault relay must be connected to an input on the SMS or to another annunciator. Figure 9 illustrates the hardware method of NMS fail detection.

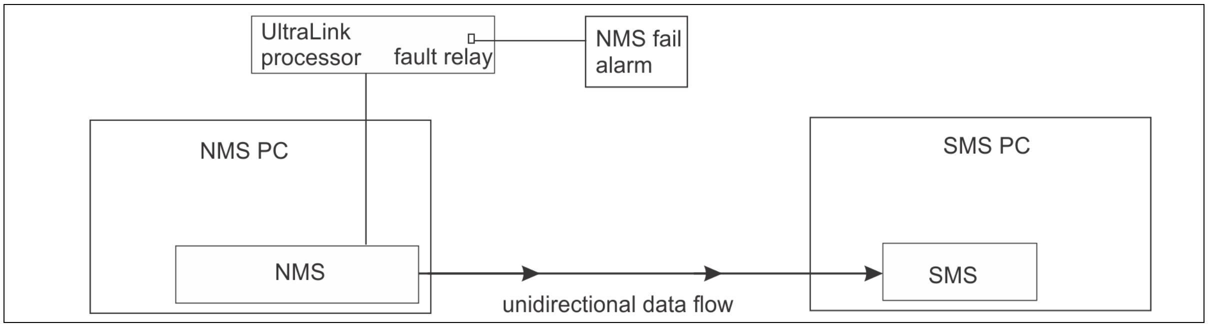


Figure 9 Hardware NMS fail indication

Redundant applications

For Network Managers requiring redundant operation, you setup two NMs on two redundant PCs (one NM on each PC). When you configure the two NMs, both are assigned the same Unit ID. In addition to the standalone configuration information, you specify the IP address of the Mate NM, and identify one of the NMs as the Primary. The first unit started is the active NM, with the second unit started operating in standby mode. If both units start simultaneously, the Primary unit is active. If the active unit stops for any reason, the standby unit becomes active after a brief timeout period. When the failed unit comes back online, it operates in standby mode. If the active unit cannot communicate with any security devices it will transfer control to the standby unit after 60 seconds. Only the active NM will accept a connection from an SMS. A standby NM will not accept a connection. Therefore, the SMS must search between the two specified IP addresses to find the active NM. If the SMS loses a connection to the active NM, it must restart the search for the active NM.

Once the Active/Standby pair is configured and communications between the two Network Managers is established, all configuration and status changes made to the Active Network Manager are synchronized to the Standby Network Manager. This includes configuration changes made through the Network Manager Front Panel, and alarm shunt and control point status changes made through the Network Manager Interface.

Figure 10: illustrates a redundant Network Manager setup. For a redundant Silver Network with a loop topology, two Network Interface Units are connected to the Silver devices. One NIU is connected to the first redundant PC, and the second NIU is connected to the second redundant PC. Both redundant PCs are running the Network Manager. The two NM PCs are connected through a hub to a Security Management System. For a redundant Silver Network with a star topology, the two NM PCs, the Silver devices and the SMSs are connected through a hub. The setups for the FiberPatrol, CCC, Crossfire, Krypton, Sennet, Sentrax, Starcom, VoE and MX networks are also indicated. For the FiberPatrol, Krypton and Voice over Ethernet networks, no additional hardware is required, as the redundant setups already require a hub/router. For the CCC network, two USB to 485 converters (OR EIA-232/485, OR Ethernet/485 converters) are used to connect to the PCs. For the Crossfire network, two redundant Switcher/Data Converters (one per PC) connect to the PCs via EIA-232 serial ports. For the Sennet network, the dual-ported Network Controller connects to both PCs via EIA-232 or Ethernet (through a converter). For the Sentrax network, the dual-ported Control Module connects to both PCs via EIA-232, or Ethernet (through a converter). For the MX network, a manual A/B switch is used to switch the MX-5000 between PCs. For Starcom, a manual A/B switch may be required to switch the serial data stream. Each sensor network requires its own dedicated Network Manager.

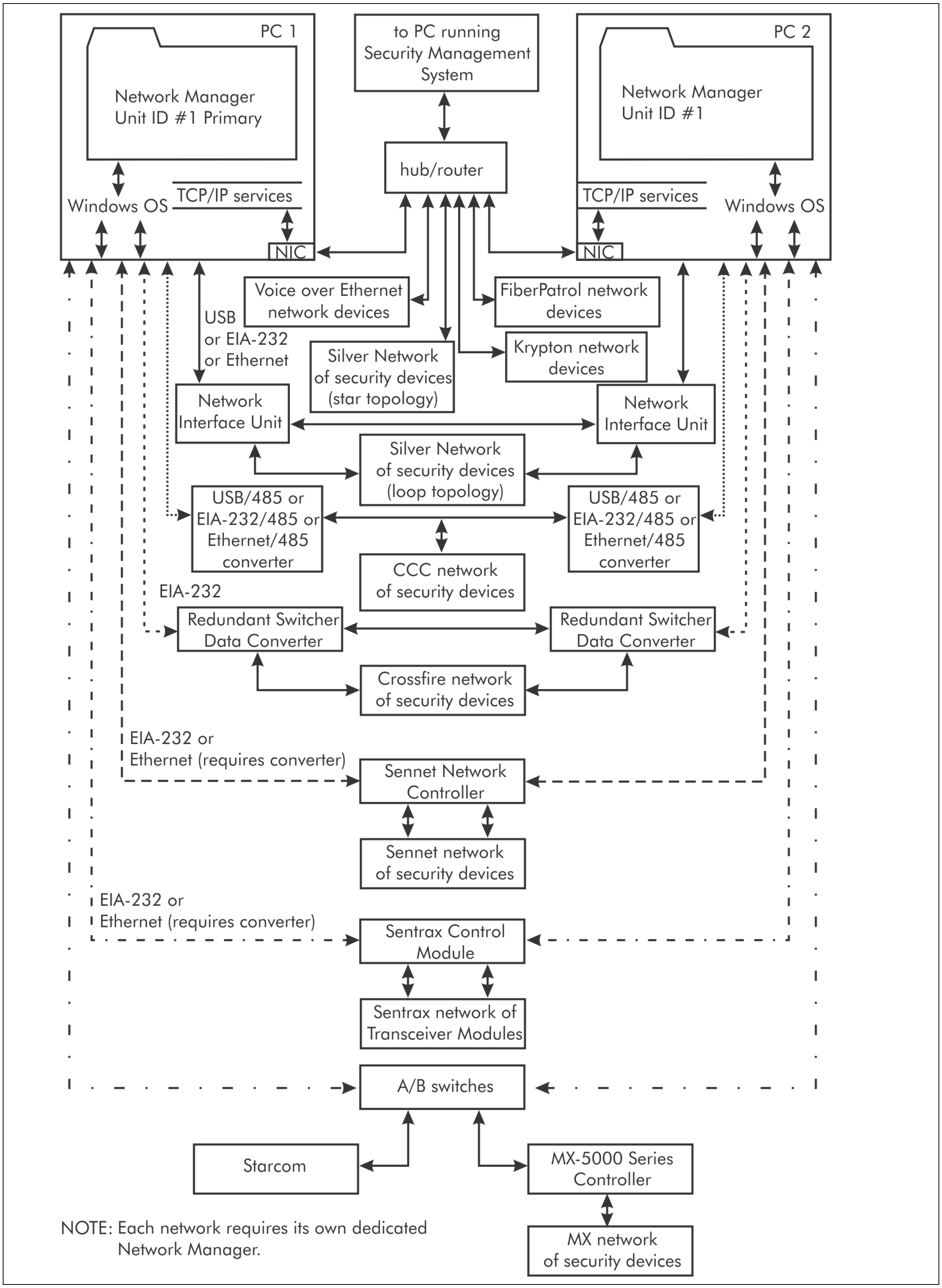


Figure 10: NM redundancy

Networking concepts

Each Network Manager can communicate with one to four Security Management Systems. The IP address of each SMS must be registered with a Network Manager in order to exchange data with the NM. The SMS connects to TCP port 849 + the NM Unit ID, at the NM computer’s IP address. This means the first NM listens for traffic using TCP port 850, the second uses 851, the third uses 852, etc. A Network Manager will not allow connections from any computer that is not on its registered list. This provides a final level of protection against access from unauthorized computers. Third party security tools such as VPNs and firewalls should be used as the primary method of protecting the network computers.

The Network Manager Interface can communicate via a TLS encrypted socket. Checkboxes located on the Front Panel SMS Config tab next to the IP fields can be used to enable, or disable, TLS on that interface. There are two files required for TLS encryption, a Certificate file and a Key file. The NMS ships with default versions of both of these files located in a “Certificates” folder in the Network Manager installation directory (default: C:\Senstar\Network Manager\Certificates). The Certificate file is named MyCertificate.pem and the Key file is named MyKey.pem. These can be replaced with site specific Certificate and Key files as long as they have the same names.

If you are using anti-virus software, you may have to setup an exception to enable the installation and running of the Network Manager Service (NMService.exe). Consult the anti-virus software documentation, or contact your system administrator for details on how to setup an exception.

If you are using firewall software, you may have to define rules to allow the necessary network connections to and from the Network Manager:

- Front Panel connection (Front Panel Port # 820 - 829)
- Security Management System connection (TCP Port # 850 - 859)
- UCM or NM Plot Tool connection (TCP Port # 830 - 839)
- NM Event Log or Status Tool connection (UDP Port # 830 - 839)
- Redundant NM connection (TCP Port # 870 - 879)

Network requirements

Computers using the NMI can be connected on any physical medium supported by the computer’s NIC hardware. This is typically a 100BaseT Local Area Network (LAN). Security Management Systems can be located outside of the LAN, and reached through the services of a gateway device (router) provided the SMS’s IP address and TCP port numbers remain the same. Security Management Systems using the NMI cannot be located behind a Network Address Translation (NAT) firewall, which alters the TCP and IP values of the outgoing packets of data. All computers (Network Manager computers, Security Management System computers) using the NMI must be configured with a fixed IP address. No address restrictions apply. The use of the private “non-Internet routable” addresses (e.g., Class C, Private Range 192.168. x.x) are recommended for added security against inbound traffic from Internet hosts. Do not use DHCP address assignments as the Network Manager requires fixed IP addresses for station identification and restriction. Note that TCP/IP communication is used both for single computer applications where the SMS and the NM are on one computer (see Figure 7:) and when a computer network is employed (see Figure 8:).