



Facts

- Availability of affordable technology has supported the expansion of the monitoring applications into industrial, institutional, commercial and municipal settings.
- Reliability and bandwidth are key factors to the success of any surveillance implementation.
- Market experts predict that 2011 is the year that IP cameras will surpass CCTV cameras as the dominant equipment for security and monitoring applications.
- Human safety and property security are top reasons cited to employ monitoring system. Process control monitoring and remote management increasingly named as decision points for new systems.

Using Ethernet to Create Highly Reliable Wide-Area Security, Access & Monitoring Systems

More and more organizations are safeguarding themselves by adding comprehensive security, surveillance and electronic access systems to their campuses and properties. The proliferation of these systems, on both public and private land, has grown exponentially in recent years. These systems can now be found in office parks, industrial complexes, college campuses, retail centers, public transportation hubs, and other places where security is a high priority.

While the wide-spread availability of security products (cameras, intercoms, access control devices, alarms, control systems, etc.) has fueled growth, they have also complicated installations. Expert planning is essential. The first challenge is to make sure that all devices share a common communication platform. Ethernet is the natural choice. It is a proven communication protocol that provides fast, reliable service. To guarantee maximum reliability, serious consideration must also be given to network topology, appropriate bandwidth and system redundancy.

**N-TRON 7506GX2
Industrial Ethernet
Switch**



White Paper Series

Campus Security / Wireless Access Applications

Star Topology

The star network configuration is always the most efficient way to design a small security network topology with wireless access. It is a very simple design allowing the use of unmanaged switches in the field tied directly to a central switch with a high-speed backplane. The fiber optic ports in this example can be used to connect to field switches up to 80 KM from the monitoring station. Power over Ethernet (PoE) switches in the field will provide both communications and power to PoE-capable devices via a single CAT5 cable.

Figure 1

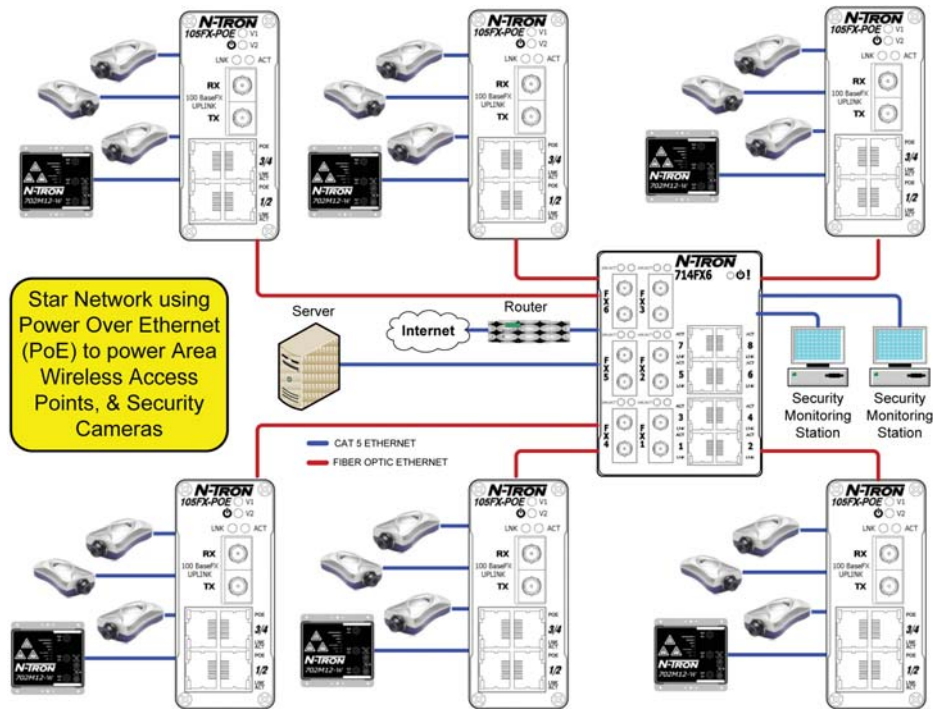
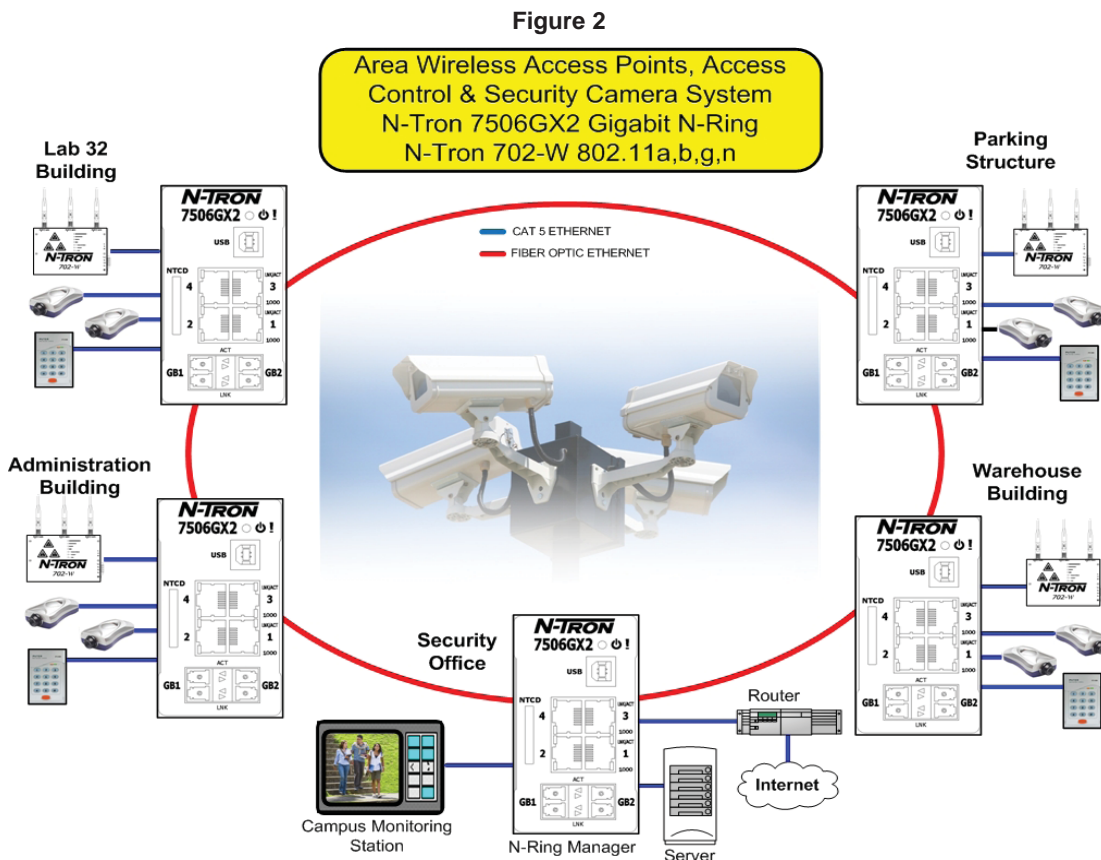


Figure 2 depicts a typical redundant ring topology used for a campus-wide system. The system includes building access control, wireless entry points to public and private areas throughout the campus, and property surveillance via IP cameras.



Ring Topology

The gigabit fiber optic ring ensures electrical isolation between buildings and provides the proper bandwidth to support cameras and wireless access points. The ring topology also provides redundant communication paths in the event of the loss of a fiber link.

System monitoring is accomplished through switches deployed within the ring. These devices use either Rapid Spanning Tree Protocol (RSTP) or a high-speed proprietary ring control protocol like N-TRON's N-Ring (30ms break detect) to send Ethernet heartbeat packets around the ring. The designated ring manager blocks one of the ring ports so that all traffic, with the exception of the heartbeat packet, will be routed through the other port.

This prevents a loop from being formed that would cause continuous recirculation of packets. Unchecked loops will eventually create a network storm ending all communications. Heartbeat packets are allowed to pass through the blocked port and are timed by the ring manager to ensure that the ring is intact. The ring manager detects a break in the system if the heartbeat packets are not received on time. It will open the blocked port in response. This allows communication to continue around the unresponsive link. When the link is restored, the ring resumes normal operations with one blocked port to prevent a loop.

White Paper Series

N-TRON switches have a convenient method of monitoring system status using the N-Ring high-speed ring management protocol. Figure 3 shows views from the N-TRON N-Ring web browser in normal and default modes. The fault status is indicated in red and will pinpoint the location of the link break. In this case, the break occurs between Switch 1, Port A2 and Switch 2, Port A2.

N-Ring OK!!					
N-Ring Status View					
Switch is an N-Ring Manager.					
Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	00:07:af:ff:f6:e0	192.168.1.136	255.255.255.0	N-TRON Switch	A2 A1
1	00:07:af:ff:f6:40	192.168.1.131	255.255.255.0	N-TRON Switch	A1 A2
2	00:07:af:ff:f6:60	192.168.1.132	255.255.255.0	N-TRON Switch	A2 A1
3	00:07:af:ff:f6:80	192.168.1.133	255.255.255.0	N-TRON Switch	A1 A2
4	00:07:af:ff:f6:a0	192.168.1.134	255.255.255.0	N-TRON Switch	A2 A1
5	00:07:af:ff:f6:c0	192.168.1.135	255.255.255.0	N-TRON Switch	A1 A2

Figure 3: N-Ring Manager Ring Status via WEB Browser

N-Ring Fault!					
N-Ring Status View					
Switch is an N-Ring Manager.					
Switch No	MAC Address	IP Address	Subnet Mask	Name	Ports
RM	00:07:af:ff:f6:e0	192.168.1.136	255.255.255.0	N-TRON Switch	A2 A1
1	00:07:af:ff:f6:40	192.168.1.131	255.255.255.0	N-TRON Switch	A1 A2
2	00:07:af:ff:f6:60	192.168.1.132	255.255.255.0	N-TRON Switch	A2 A1
3	00:07:af:ff:f6:80	192.168.1.133	255.255.255.0	N-TRON Switch	A1 A2
4	00:07:af:ff:f6:a0	192.168.1.134	255.255.255.0	N-TRON Switch	A2 A1
5	00:07:af:ff:f6:c0	192.168.1.135	255.255.255.0	N-TRON Switch	A1 A2

Network Monitoring Applications

N-TRON Managed Switches also provide an OPC-based monitoring tool (OLE for Process Control) which reports more than 40 different performance parameters on each port and 10 per switch. The OPC server software, N-View, can be used as a standalone monitoring tool or can integrate into most Windows-based HMI and SCADA systems. An example of this can be seen in Figure 4.

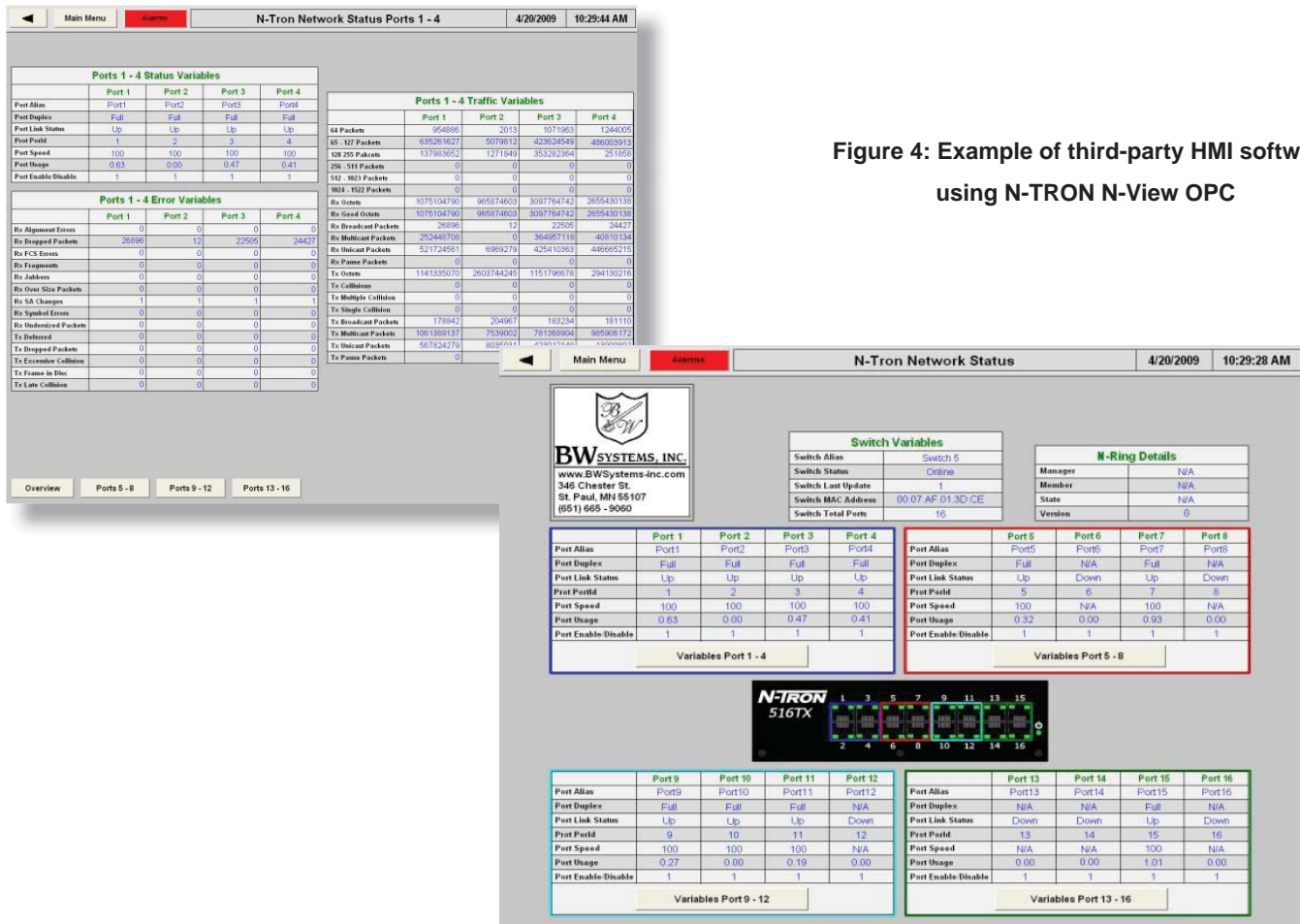


Figure 4: Example of third-party HMI software using N-TRON N-View OPC

Switch Specifications

Switches used in these applications are subjected to environmental challenges not found in ordinary IT installations. They are often exposed to harsh and unusual conditions and must provide uninterrupted service for extended periods of times. Only the most durable, proven devices should be used for these installations. The following environmental and reliability specifications should be considered:

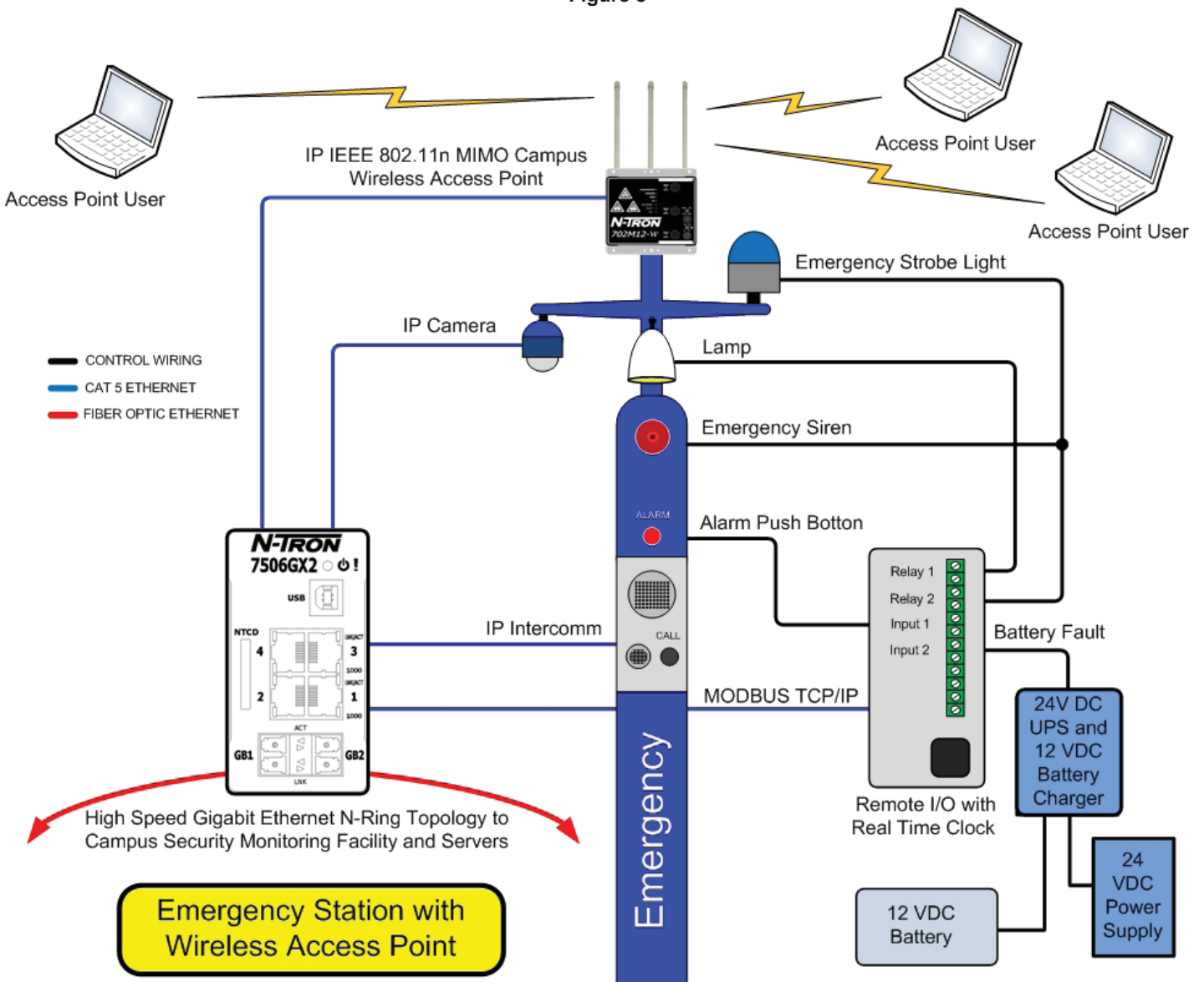
- -40° to 80° centigrade operation
- 50g vibration
- 1 million hours mean time between failure (MTBF)
- 200g shock
- 15 kV ESD overvoltage protection

White Paper Series

Emergency Station Applications

Durable switches are mission-critical for emergency alert systems such as remote police/fire/medical call stations. Used to contact first responders, these compact, self-contained systems are commonly found throughout campuses, business centers, parks and recreational areas, as well as other municipal settings. Figure 5 provides a snapshot of this application. In this instance, the system uses 24 VDC-powered devices with a DC UPS backup to maintain power in the event of an electrical outage.

Figure 5



Emergency Station Components

The emergency station components include:

- Managed gigabit switch with high-speed ring management and OPC monitoring.
- A MODBUS TCP/IP remote input and output module with real-time clock. This component allows security personnel to control sirens, strobe lights and lamps at the scene or from a remote location. It also sends an instant message to the master control center when an alarm button is pushed or when the UPS battery has a problem. The real-time clock records these events and can also be used to set on/off times for system lamps or spotlights.
- IP intercom for emergency two-way communications with security personnel.
- IP camera for area surveillance.
- IEEE 802.11 a, b, d, n wireless access provides wireless service to the surrounding area.
- LED lamp used to light the emergency station.
- Siren and emergency strobe light for emergency alert.
- Alarm push button to signal security personnel that an emergency is underway.
- 24 VDC power supply.
- DC UPS and 12 VDC battery charger (see PULS UB10.241).
- 12 VDC rechargeable battery.

N-TRON 702-W
Wireless Radio



White Paper Series

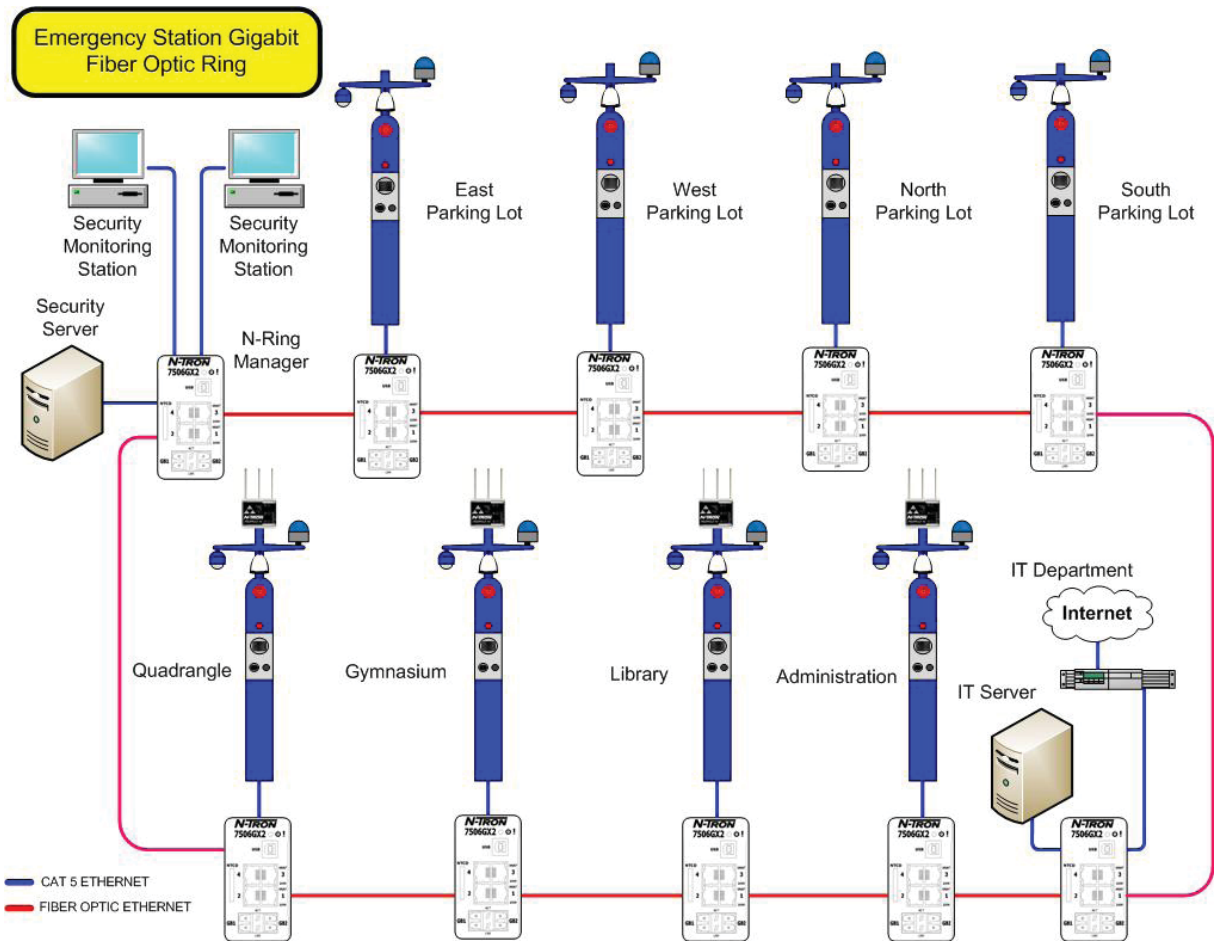
Networking Stations

Stations are normally secured and interconnected through a high-speed fiber optic ring. The fiber optic cable and transducers on each switch must match. Links less than 300 meters can use multimode fiber optic cable and switch transducers at each end of the node.

Links over 300 meters should use single mode fiber optic cable and single mode switch transducers. Please note—these two fiber cables are not compatible so the network should be planned with this in mind.

The choice of the cable should be done with the advice of a vendor with a full understanding of how the cable will be deployed and the exact distances between each link. The switch provider should be told the type and length of cable so they can provide the proper transducers for the application. The fiber optic cable must be terminated to match the type of termination required for the transducers used.

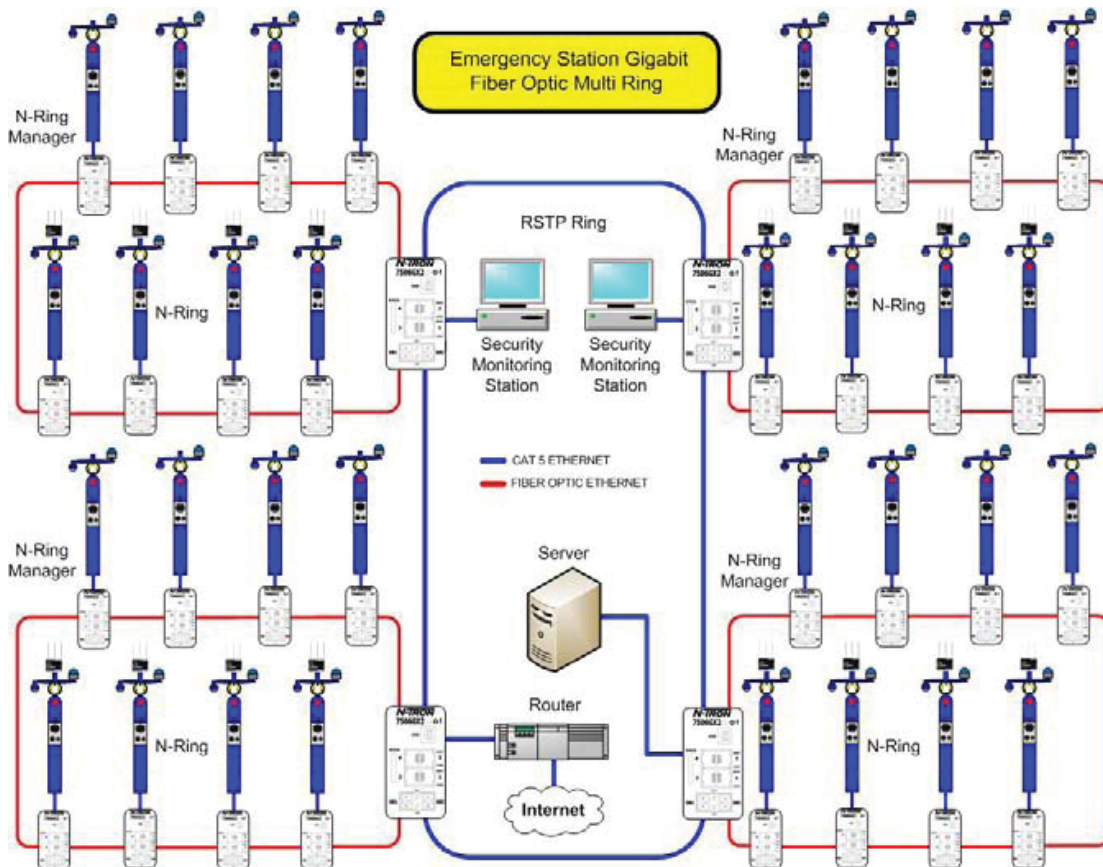
Figure 6: Example of single ring station deployment



Large or Multiple Ring Networks

Larger geographic areas may require a multiple ring solution. Figure 7 depicts four high-speed N-Rings tied into a central control center network running RSTP.

Figure 7



This type of topology must be planned carefully due to the sheer number of devices involved in an installation. Two critical elements are needed to complete this system—adequate bandwidth and sufficient IP addresses to handle the volume of devices.

Bandwidth issues can be solved by limiting the number of devices on the network or by using separate monitoring stations for each ring. Servers can be configured to provide more bandwidth through the use of multiple network interface cards (NICs)—one per ring. Larger networks may need more IP addresses than the 254 available in one subnetwork.

These installations may also need to segment security areas into separate networks using virtual local area networks (VLANs) so that IP addresses can be reused in each area. The N-TRON VLAN function allows each port in a switch to be set to a separate VLAN ID. The switches in the main control room ring can be used to segment the network into VLANs. This configuration allows the use of duplicate IP addresses in each VLAN.

White Paper Series

Did you know?

N-TRON® is recognized around the world for developing and manufacturing high-quality ruggedized products for Industrial Ethernet automation. The company's network solutions are the benchmark for quality and reliability, providing exceptional performance for mission-critical data acquisition and control applications. N-TRON offers a complete line of affordable unmanaged and managed Ethernet switches, media converters, Power over Ethernet (PoE), and wireless access devices for industrial environments.

Other Protocols to Consider

Quality of service (QoS) allows voice over IP and video over IP packet prioritization. These applications require QoS to deliver voice and video without gaps in delivery due to packet buffering delays on the network. Most IP cameras and IP intercom systems use multicast messaging requiring each switch in the network to be able to route these messages properly using Internet Group Management Protocol (IGMP Snooping). N-TRON managed switches automatically use IGMP Snooping to manage the group multicasts messages created by these devices.

Because these systems run software that use the IP addresses of field devices for communication (examples—to view camera feed, call the intercom, etc.), a change to the address means an update to system software. This problem is avoided if Dynamic Host Configuration Protocol (DHCP) Option 82 Relay switches are used to load the original address. DHCP Servers and Option 82 Relay switches can be configured to provide a specific IP address to a particular device connected to a specific port of an Option 82 Relay switch. This allows hassle-free field replacement of IP devices such as cameras or intercoms, since the new device is automatically assigned the same IP address as the previous one.

Note—To use Option 82 Relay addressing, field devices must be setup as DHCP Clients.

N-TRON USA & Corporate Headquarters
820 S. University Blvd • Suite 4E
Mobile, AL 36609 • USA
Phone 251-342-2164
Fax 251-342-6353

www.n-tron.com

N-TRON ASIA PACIFIC

CHINA
Phone +86-021-6194-6777
Fax +86-021-6194-6699

INDIA
Phone +91-9844-876540

SINGAPORE
Phone +65-8118-6821

N-TRON EMEA

Phone +41-41-740-6636
Fax +41-41-740-6637

N-TRON UK/Ireland/Nordic/Benelux

Phone +44 (0)1928 577257
Fax +44 (0)870 7051506