Moxa White Paper

Real-time Video Monitoring Increases the Efficiency of SCADA Process Management

Harry Hsiao, Moxa Product Manager
(harry.hsiao@moxa.com)

Traditional SCADA (Supervisory Control and Data Acquisition) systems have been an important part of automation control systems for many years, and although SCADA systems come in many shapes and sizes, they are all designed to monitor and control the status of devices and processes. In the past, SCADA systems relied solely on numbers and text to monitor the status of a system and formulate appropriate responses. In a very real sense this left human operators in the dark since they had no way of viewing the source of a problem without spending the time and effort needed to go onsite. Recent developments in video networking technology are making it possible for operators to monitor field sites from a central control room, and in the process maintain a much tighter control over their operation.

What is SCADA?

A typical SCADA system is used to automate complex industrial processes in situations where human control is impractical. Examples include monitoring remote unmanned sites, systems with many complex and fast-moving control factors, and environments that are not suitable for humans. SCADA systems are used for a wide variety of applications.

Released March 2008

Moxa manufactures one of the world's leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial cards, embedded device servers, and remote I/O products. Moxa's products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

- **Oil and gas wells, refineries, and pipelines**—Use a SCADA system for remote monitoring and control of facilities and equipment to ensure a smooth production process and operational safety.
- **Electric power generation, transmission, and distribution**—Electric utilities use SCADA systems to detect current flow and line voltage, monitor the operation of circuit breakers, and take sections of a power grid online or offline.
- **Water and sewage**—State and municipal water utilities use SCADA systems to monitor and regulate water flow, reservoir levels, pipe pressure, and other indicators.
- **Buildings, facilities, and environments**—Facility managers use SCADA systems to control HVAC, refrigeration units, lighting, and entry systems.
- **Manufacturing**—SCADA systems manage parts inventories for just-in-time manufacturing operations, regulate industrial automation and robots, and monitor processes and quality control.
- **Mass transit**—Transit authorities use SCADA systems to regulate electricity to subways, trams, and trolleys, automate traffic signals for rail systems, track and locate trains and buses, and control railroad crossing gates.
- **Traffic signals**—SCADA systems are used to regulate traffic lights, control traffic flow, and detect malfunctioning traffic signals.

SCADA systems let you do more for less, and as a result increase your profit.

SCADA systems help system operators make well-informed decisions about their system. Sensors and actuators can be placed at each of a managed processes critical points to provide a detailed view of operations as they occur. SCADA systems offer a real-time and comprehensive view of all events, even for very complex manufacturing processes and large electrical plants, and provide the information needed to correct errors and improve efficiency. SCADA systems let you do more for less, and as a result increase your profit.

The four main functions of a SCADA system are:

- Data acquisition
- Networked data communication
- Data presentation
- Control

Many I/O devices (such as sensors, RTUs, and PLCs) are used for data acquisition and control, and data transmission through a network. However, I/O devices only transmit numbers and words, and as such cannot offer a complete picture of what's happening at a field site. For example, if an abnormal temperature is detected and reported to the SCADA system, the temperature and alarm message may be the only data presented, and consequently it may be impossible to determine the cause of the event. In this case, system operators need to ask field engineers to go onsite to evaluate the situation and find a quick fix for whatever is causing the problem. However, in some situations it may be impossible for the field engineers to find a solution, and there may also be unexpected dangers, such as fire.

Integrating a Video Networking Surveillance Application into a SCADA System

A new trend is to integrate real-time video surveillance into SCADA systems to give system operators a more powerful tool for managing their processes. The main goals of including real-time video are:

- Be able to see what's happening onsite in real-time, even if no one is at the field site.
- Save time and labor by being able to view equipment and the environment from off-site.
- Give engineers better information about dangers at the site before sending them to the field site.
- Record events in real-time, even when it is not possible to check in person.
- Prevent sabotage and theft.

Networks for modern SCADA systems are migrating to Ethernet-based TCP/IP to provide better remote accessibility, integration capability, and easier deployment and management. Following this trend, many I/O devices can now connect directly to an Ethernet network for greater data transmission versatility.

This Ethernet-ready trend also applies to video surveillance devices. However, due to the complexities of video digitization and compression technologies, and the variety of video networking solutions on the market, system integrators may have trouble selecting and integrating suitable video networking solutions into their SCADA system. In addition, system integrators must consider how environmental conditions may affect the system, and then choose products accordingly.

Thanks to advances in video digitization and compression technologies, video networking surveillance is becoming the mainstream of video surveillance systems. Many video networking solutions, such as IP cameras, video servers, and NVRs (network video recorders) are being developed to implement networked video surveillance systems. By using such devices system integrators can easily integrate video surveillance applications into their SCADA system. Four factors must be considered when choosing which video networking solution to use for your SCADA system:

- Applicability
- Reliability
- Integration
- User-friendliness

Applicability—choosing the right video networking product is a must to ensure smooth operation and reliability

Along with recent developments in video-over-IP technologies and solutions, many advanced functions, such as H.264 video codecs, mega-pixel resolution, and IVS (intelligent video surveillance), are provided for enhancing video quality and video intelligence. However, system integrators must determine if these functions are suitable for their SCADA

system. Since video surveillance applications serve as auxiliary monitoring systems in SCADA systems, the video surveillance system should not influence the main I/O monitoring and control operations. Whereas advanced functions offer more system complexity, they demand greater system resources and may affect the overall performance of the system and network. For this reason, system integrators should consider the requirements of both video surveillance and overall system performance when creating the optimal video networking surveillance system.

In addition to obtaining the optimal video networking surveillance system, the hardware installation of video-over-IP devices also needs to be considered, since field sites could be subject to harsh environmental conditions, such as high temperatures and high humidity. To ensure that devices operate as expected, a cabinet or 19" rack is often used to protect the hardware.

Reliability—redundancy, high MTBF, wide operating temperature, and rugged enclosure are all important factors to consider

There is no doubt that reliability is one of the most important considerations when choosing a video networking surveillance solution to use with your SCADA system. Harsh environmental conditions, such as low or high temperatures, humidity, EMI, and surge, give system designers a big challenge when choosing which devices and equipment will be used with their SCADA system. Pay attention to the following key points when choosing products:

- **Redundancy**—Redundant solutions, such as redundant power and redundant Ethernet, guarantee non-stop operation of systems and devices.
- **MTBF (Mean-Time Between Failures)**—The MTBF value is the average time between failures for a device. A higher MTBF value indicates that a device is more reliable.
- **Surge and EMI protection**—Most SCADA application environments are likely to be subjected to severe electrical and magnetic influences. In order to protect electronic devices, higher EMI and surge protection are essential.

- **Operating temperature**—Some SCADA applications require products that are guaranteed to operate in wide temperatures ranges that could start as low as -40°C and range as high as 75°C. For these types of applications, it is important to look for products that do not use built-in fans, since products with fans tend to have a lower MTBF.
- **Enclosure protection**—A rugged design provides good physical protection against unexpected damage from external factors. The Ingress Protection (IP) rating index (EN60529) is an international classification system that rates how well electrical equipment is protected against the intrusion of foreign objects (e.g., tools, dust, fingers) and moisture.
- **Product warranty**—A good warranty helps ensure that you can keep your maintenance costs at a minimum.

For video networking surveillance solutions, system integrators of SCADA systems should look for the products that meet the above criteria.

Integration—creating an integrated system for centralized control of distributed devices takes careful planning

By their very nature, SCADA systems are highly integrated and centralized. Many devices and equipment at field sites are monitored remotely and controlled by system software from a central location. The relative ease or difficulty of system integration determines the amount of time and money that must be invested for system development and installation. There are three aspects to this issue that should be considered:

- **One Network**—For integrated systems, devices and equipment must be connected to one network topology. Ethernet TCP/IP networks can accept a wide variety of I/O monitoring and control devices and equipment (at least those with versatile connection interfaces) in one network. Not only data, but also video and voice, can be transmitted over TCP/IP networks, allowing SCADA system networks to be implemented in one network topology.
- **One System**—One of the key issues of integration is that you will need to monitor devices and equipment that use

different data transmission protocols, such as analog I/O, digital I/O, and Modbus, in one system. Video networking transmission uses a digitized and compressed video stream with specific algorithms (motion JPEG and MPEGx, for example), usually involving proprietary technologies. Therefore, it is essential to get an SDK (software development kit) or API library from the video networking solution supplier when integrating video surveillance into a SCADA system. Most SDKs provided by video networking solution suppliers include the ActiveX Control component, which can be used as a plug-in object on a web page, and SCADA software to decode and display the video stream. Some SCADA software directly supports the ActiveX Control object, so system integrators only need a few steps to build a video display into the system.

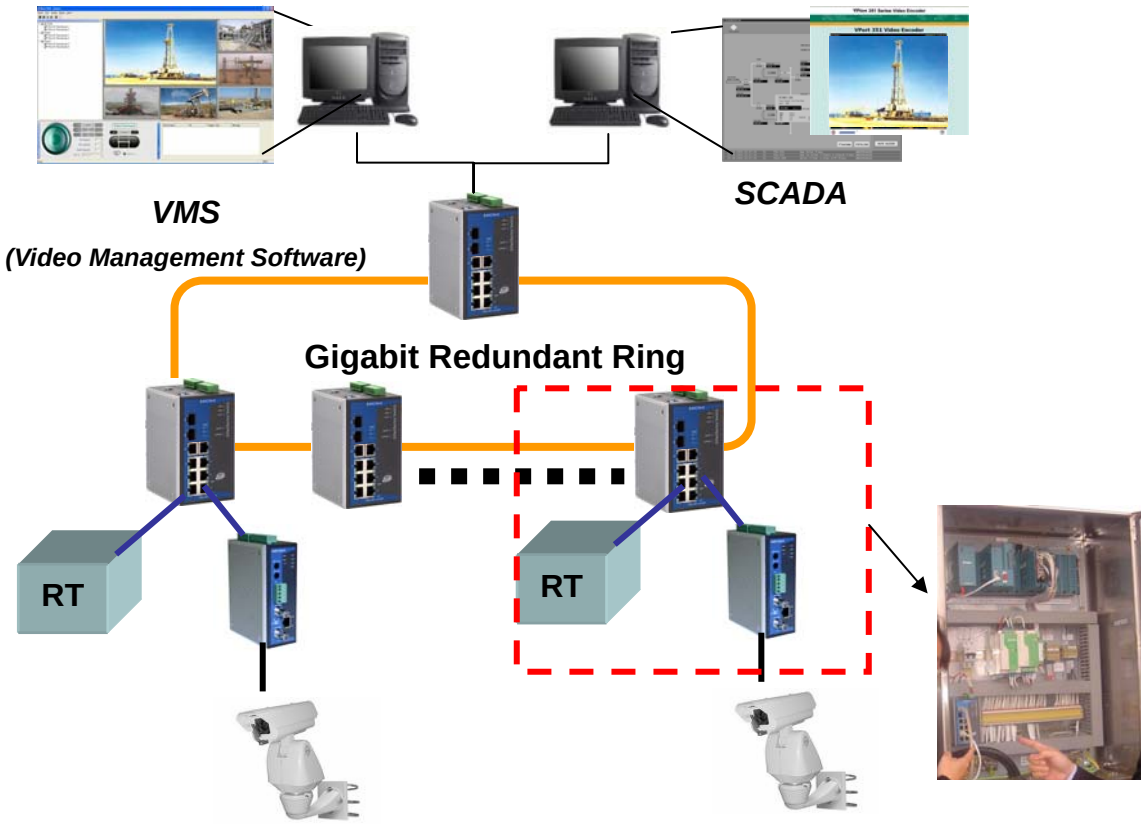
- **Interoperability**—If system integrators want to implement interoperation between data and video, such as automatic video display when an event occurs, then interoperability should be considered. Currently, SNMP network management protocol is the most popular tool for TCP/IP Ethernet networks, and can be used to monitor the status of devices and equipment, and trigger a control action when an event or alarm occurs.

User-friendliness—using video surveillance systems that are easy to use is a must

Since including video networking surveillance systems with SCADA systems is a new trend, most system integrators and operators are not very familiar with the technology. To make video networking surveillance systems more accessible to users, it is important to simplify installation and operation, and make the user interface similar to the interface used by the SCADA system.

Reference Case: Video networking application combined with SCADA software for oil well monitoring & control system

Most oil wells are located in remote areas that are subjected to harsh and critical weather conditions. The SCADA system in this example is used to monitor and control field site equipment to ensure that the site operates normally. To make monitoring more efficient and also save labor costs, a leading oil company in Saudi Arabia decided to implement a video networking system to help monitor field site equipment and weather conditions.



Video networking applications play a major role in helping SCADA administrators monitor filed site situations using actual video images. Video management software is used to display the video images, which can also be displayed on the SCADA server when operators are faced with an emergency situation. By using actual video images, operators can know immediately what has happened at the field site, and then make the right decision on how to handle the problem.

Summary

Although a variety of video networking surveillance solutions for real-time monitoring are available on the market, SCADA system integrators should choose the optimal solution, based on applicability, reliability, integration, and user-friendliness. In addition, SCADA systems are highly integrated, with many devices and equipment connected to one network, and managed from a central location. For this reason, advanced planning and a clear vision of the system architecture are required to ensure successful integration of the SCADA system. Since some SCADA system integrators are often not very familiar with video networking surveillance systems, it is a good idea to find a qualified consultant, or even a complete networking solution provider, to help with system and network planning.