A ROBUST MIDDLEWARE ARCHITECTURE FOR INTELLIGENT DATA AGGREGATION AND VIDEO SURVEILLANCE

Tamer Mohamed[1], Mohamed Shehata[1,2], Wael Badawy[1]
[1]IntelliView Technologies Inc.
Calgary, AB, Canada
[2]Benha University
Cairo, Egypt

Abstract

Typical video surveillance systems are very demanding in terms of infrastructure required to deploy them and also in terms of human resources required to operate them on a continuous basis. In this paper, we propose a system architecture that aims at addressing both issues. The system is composed of multiple intelligent nodes that acquire, process, and archive data/video at a remote site and then automatically generate either alerts or summary reports that are sent to a station at the central operations office of the customer. The intelligent nodes are capable of analyzing multiple types of input data, including video, and take actions ranging from communicating alerts back to the human operator to automatic shutdown of a complete facility. These intelligent nodes serve as the middleware devices in this distributed architecture. We present a case study in the pipelining industry in Canada.

Introduction

Control operations of a remote facility have the following generic requirements: Video Surveillance, Personnel access control, Data collection from instrumentation and various gauges, and Remote control of actuators, door locks, alarm systems … etc. Deployment of these systems is very demanding to the facility infrastructure because it involves installation and wiring of heterogeneous types of networks and wiring it all to a central operations office or a control room. Another disadvantage is the requirement that human operators continuously monitor information coming from these systems using different monitoring stations. It is possible to automate some of the operations. However, the flexibility of doing this can be greatly enhanced using our proposed architecture which consolidates the required management and data aggregation in one middleware device. This device is programmed via an intuitive user interface which categorizes the relevant information and provides consistent ways for managing a facility or a section of it.

System Architecture

The central part of the system acting as the middleware device is an embedded ruggedized processing unit with no movable parts to survive harsh environments.

This device has analog video capture capabilities, RS485 interfaces and several networking options. The hardware additions to this system are the following:

1. A data acquisition card for data collection and control of gauges and actuators in the remote site.
2. Door access controllers networked via the RS485.
3. Analog cameras networked via dedicated cables or IP network cameras or both.
4. Interface to SCADA systems.

In a typical architecture, known as central server based, all video and sensors data are communicated back to the central station where they are fully analyzed. In our proposed architecture, we introduce the use of our middleware device to do all processing and analysis at the node and only communicate when there is a threat to the operation of the system (e.g., intruder in the area). Table 1 shows a comparison of both architectures.

Table 1: Distributed Architecture vs. centralized one in remote site management with video surveillance.

	Central Server Based Architecture	Distributed middleware Architecture
Advantage	Simple to design. Easy to install. Easy to maintain. Easy to secure data	Reduce installation Cost Camera Collaboration. Low bandwidth. Automation. Modular expansion. Video analytics. More Reliability.
Disadvantage	High installation cost. High expansion cost. High bandwidth usage	Power management. Data security at remote site.

This middleware software architecture is based on a modular architecture to allow maximum flexibility. The software modules are:

1. A video analytics engine with a host of video based detections including object tracking, face detection, license plate logging and vehicle counting.
2. A Modbus data collection programming.
3. Data acquisition programming.
4. Door access control programming.

5. Programmable Power management for multiple power sources including fuel cells, solar panels and rechargeable batteries.
6. User defined policies for detection of events based on information from both exclusive and inclusive scenarios and acting upon them.
7. A data communication module for remote programming via a dedicated client or a web interface.

CASE STUDY

There are new requirements for monitoring and recording activity within the energy industry. They are in different phases of implementation or enforcement, but they demonstrate an operational shift in the industry [2]. For example: On August 2009, the Canadian Standards Association introduced the CSA Standard Z. 246.1 E9 – Security Management for Petroleum & Natural Gas Industry Systems standard [1]. This is a Canadian and North American first and it was immediately put into action by some governmental agencies [3].

The new CSA standard had been developed in response to the increasing threats of vandalism and sabotage to oil and gas pipelines. It has been designed to help the pipeline industry secure their assets while protecting public safety**.** Our proposed solution leverages existing infrastructure and minimizes the deployment costs for newer sites.

Description

This project involved securing the perimeter of a sour gas control head. The proposed solution combines personnel access control, a night vision camera and motion detectors. Power for the system is provided via a solar panel. The system generates image evidence and actuates an alarm siren. Monitoring of this site and other sites is via a web interface. Site specific information is overlaid on a Google maps based interface as in Figure 1. Data updates from the video analytics and the gauges are sent at a rate of 0.1 to 5 Hz depending on available bandwidth and are sent via the existing SCADA or via the integrated cellular modem.

PERFORMANCE

In this project, e-mail notification was used instead of SCADA alerts. In a period of 6 weeks, the system was completely autonomous and generated 169 messages that required verification by a human operator. The false alarm rate for the video analytics is 15%. Figure 2 shows a 2D video summarization to pinpoint anomalies in the scene.

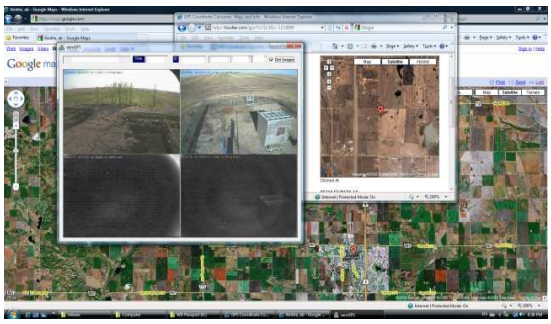

Figure 1: The system on the Google maps interface

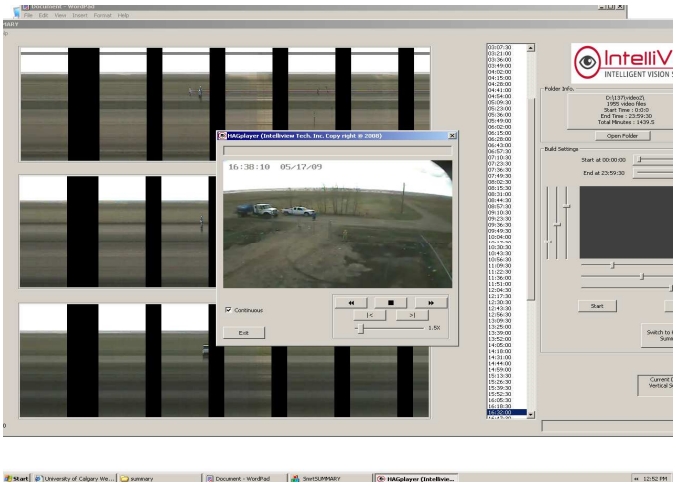

Figure 2: 2D video scene anomaly summarization pinpoints an event when two company cars parked in front of the facility.

Conclusion

Traditional video monitoring systems use banks of screens with personnel to determine if there is a security violation and require additional infrastructure investment. The proposed system simplifies the integration into existing systems and provides a single programmable node for each remote site. The case study pipeline operators meet the new CSA security requirements.

Acknowledgement

The authors would like to thank Ms. Saika Sharmeen for her major contributions in the software design.

REFERENCES

[1] CSA standard Z246.1-09, www.csa.ca
[2] Lumina Market Study 2009, oil and gas opportunity
[3] British Columbia Oil and Gas Commision, Information Letter # OGC 09-27. http://www.ogc.gov.bc.ca