Stafford General Hospital Technical Case Study

TABLE OF CONTENTS

Introduction

Most hospitals in UK deploy surveillance of some kind in and around their premises. Surveillance was generally deployed from the early 90s to help ensure the safety of staff and patients. Surveillance has been progressively tightened in response to a series of incidents including abduction of babies and scenes of violence and disturbance.

1.1 Stafford General Hospital

Stafford General Hospital is one of many hospitals deploying surveillance and has decided to implement a network surveillance system. It is based just two miles outside Stafford town centre and is part of the Mid Staffordshire NHS Trust in the West Midlands. Stafford Hospital holds an extensive outpatient area, cancer treatment unit, acute stroke unit, a post graduate medical centre, and a 24-hour Accident & Emergency unit. It also has a special care baby unit, three maternity wards and an infirm elderly unit. It employs more than 2,500 regular staff and has 450 beds. Stafford Hospital's 900 staff are supported by IT staff from the local Health Infomatics Service (HIS). HIS staff provide desktop, networking and server support.

1.2 Management of Security at Stafford Hospital

The Portering & Security Services Department of Stafford General Hospital employs 30 porters and security staff operating on a rotational basis around the clock so that at least six staff are on duty at any one time, led by one duty supervisor to enable rapid response to security-related incidents.

1.3 Renewal of the old security system

During 2001 the Portering & Security Services Department began to express concern about the quality of recorded images generated by the ageing CCTV cameras that were installed in the 80s. Simultaneously HIS IT staff wanted to get the most of its new network by running a surveillance system using new 1Gb cabling and wireless Ethernet links. In addition, both departments knew that a traditional CCTV system would involve new coaxial cabling in the main hospital and space for additional cabling was in short supply. Stafford Hospital therefore decided to call in the experts to tender for installation of a new IP-based surveillance solution in the autumn of 2001.

1.4 Appointment of Plexnet to Pilot Stage

Network security installer Plexnet was appointed in January 2002 to provide a highly reliable IP-based surveillance system producing high quality images that could be accessed by security staff via the existing network infrastructure.

Plexnet then selected Axis Communications to provide key equipment for the new IP surveillance system including video servers to convert existing analogue-based CCTV cameras and new network cameras. Axis Application Development Partner and desktop security solution provider DV Networks was also selected. DV Networks' core offering is a desktop-based monitoring solution called "DISCOVERe" which enables easy display, monitoring, recording and retrieval of images from multiple surveillance cameras.

1.5   Technical implementation

Prior to 1998, Stafford Hospital had installed a total of 16 analogue cameras, attached to a multiplexer/VCR which was based in the hospital's security office, from here all cameras could be viewed and managed. This equipment was replaced by a Digital Video Recorder later on. In February 2002 a pilot study was conducted with just four cameras (one AXIS 2120, one AXIS 2100 and two analogue cameras) all attached through an AXIS 2400 video server) to DV Networks' DISCOVERe system. After this trial proved successful the whole system was installed and rolled out in just three months, going live in April 2002.

1.6   The security system

Four AXIS 2120 network cameras were installed at the main entrances of the main building and three Axis 2100 network cameras at the Technology Park 1.2 kilometre away and linked via 11MB wireless link. One AXIS 2100 network cameras was deployed inside the main hospital. Cameras inside the hospital and the Technology Park are sited at the reception, on entrances and exits, at the special care baby unit, maternity wards, in the infirm elderly unit, and at the cardiology and acute stroke unit.

Three AXIS 2400 and two AXIS 2401 video servers were deployed to take analogue feeds generated by the 14 existing analogue cameras and digitise them before transmitting the video across the network. A total of 21 cameras were now deployed in the hospital's main building and in the Technology Park.

DV Networks' DISCOVERe version 4 was deployed to view and store security incidents. The DISCOVERe system takes images generated by multiple cameras and displays these in quad or single view on a PC monitor and saves them down to a hard disk drive of a PC in the hospital's main security office.

The DISCOVERe system also provides the ability to vary picture size, resolution and numbers of cameras being viewed on-screen. It also enables rapid retrieval of those images from the hard disk for review purposes. In addition to reviewing recordings, live images can also be displayed. Images are stored at Stafford or exported as AVI video files or BMP still images. The cameras themselves use the Motion JPEG standard for image collection[1].

Three Axis 2400 and 2401 video servers are networked with DV Networks' DISCOVERe software. The DISCOVERe software enables Giles Perry, Trust Security Manager and the person in charge of managing Stafford Hospital's security services and all related surveillance operations, to control the variable frame rate for viewing and recording to the main server. This is important because some areas where there is high traffic such as entrances, a high frame rate is crucial to ensure all people entering are captured and identifiable from the images stored. Frame rate can be lowered in areas where there is less traffic in order to restrict bandwidth usage.

Giles Perry was also able to use the DISCOVERe system to determine the number of days of recordings that could be safely stored. All camera images for the previous 15 days is stored on a DV Networks configured 960 GB RAID device (Random Array of Independent Disks) with 6 x 160GB disks operating inside a Pentium 4 1.8 750MB server. The RAID device has a 1GB link onto a Virtual Local Area Network (VLAN) dedicated to serving all cameras. All cameras except the 3 connected wireless have 100MB links into the RAID device for recording and storage purposes.

Giles Perry explained why he was happy with the 15-day limit: "In all the years I have been in surveillance I have never been asked to provide evidence of an event that was more than two weeks old". Two workstations support the system. One provides the recording to hard disk and viewing and the other provides back up storage particularly for images that may be used as evidence of a crime at some future date.

DV Network's DISCOVERe uses a graphical user interface (GUI) similar to the Calendar section of Microsoft Outlook for locating particular periods in time when events are reported to have taken place. It offers a graphical display of a monthly calendar, and time clock so the date and time can be selected based on a reported incident where the images can be easily retrieved. Because all images can be recorded at between one and 25 frames per second it is extremely rare for security to miss any incident from a suspect entering the hospital to an assault in Accident & Emergency.

1.7   Expansion of the Network into Stafford Hospital's Car Parks

As part of an efficiency drive and following the success of the IP surveillance project within the hospital itself, the trust decided to take the hospital' car park security in-house. This development led to the deployment of a further 19 external network cameras, replacing the existing analogue CCTV units.

1.8   IP Surveillance Offers Opportunities for further Integration

Mr Perry and his team hopes that over time he will be able to integrate the existing access control system with the IP surveillance system operating inside the hospital and the surveillance system covering the car parks which will now be integrated with the indoor IP surveillance system.
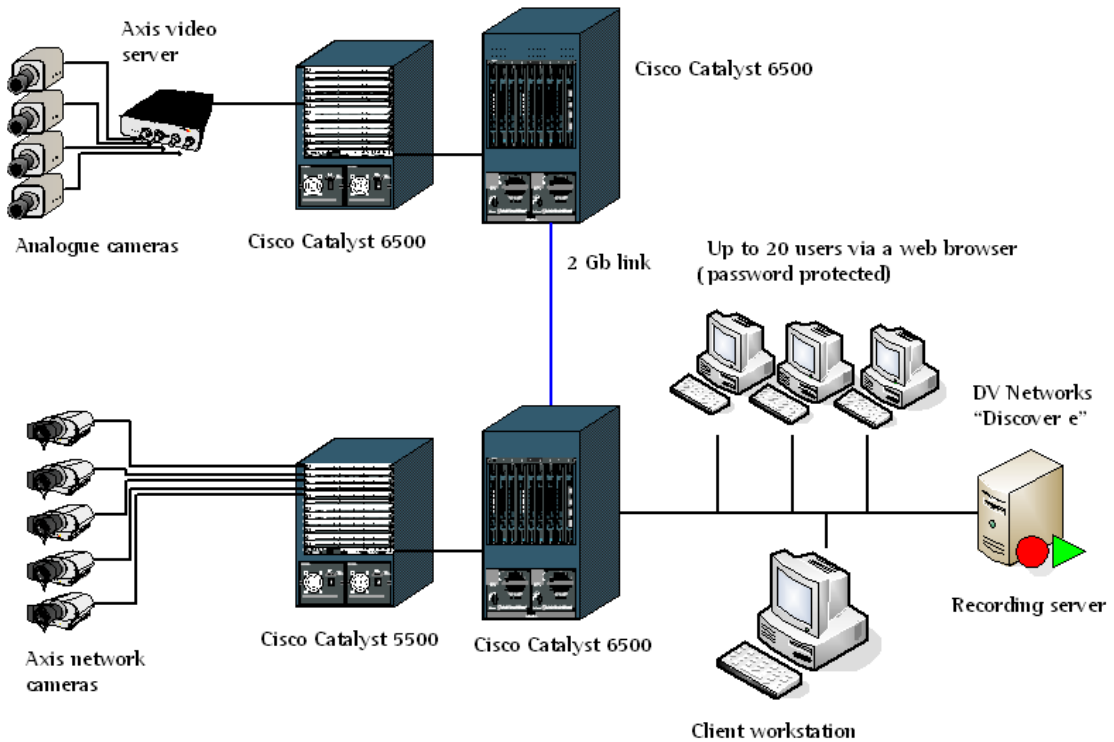
1.9 Technical Specifications of Stafford Hospital's Surveillance System:

- DV Networks DISCOVERe monitoring solution
- 3 AXIS 2400 Video Servers with 4 analogue cameras on each.
- 2 AXIS 2401 Video Servers with 1 analogue cameras on each
- 14 analogue cameras
- 3 AXIS 2100 Network Cameras - 1 recording an entrance and exit to a ward in the hospital and 2 more providing images in the Technology Park 1.2 km away. These cameras are designed specifically for indoor use offering light sensitivity to 10,000 lux and up to 10 frames per second.
- 4 AXIS 2120 Network Cameras – These cameras have built-in motion detection and use a varifocal DC-iris lens, which allow for deployment in - and outdoors.
- The widely-used standard for video usage and transmission known as Motion JPEG compression algorithm is used to ensure high image quality and frame by frame recording in compliance with Police Scientific Development Branch's (PSDB) rules on admissible evidence as detailed in the Digital Imaging Procedure document published in March 2002.

1.10 Network Infrastructure at Stafford

- Stafford Hospital operates a 1GB backbone containing two core Cisco 6500s switches with 2GB connection running between them
- These core switches link to 20 Cisco 5500 edge switches
- The entire network is configured as a number of Virtual Local Area Networks (VLANs) routed via on-board Multi Switch Feature Cards (MSFCs) operating inside the core switches on the supervisor board
- All cabling within the hospital is 1GB manufactured by Avaya and comes complete with 25-year warranty
- Stafford currently uses Omnetica for supply, installation, integration, testing and upgrading of all Cisco equipment. Plexnet currently supplies and fits all cabling.

1.11 Conclusion

Stafford General Hospital has implemented a networked surveillance system inside its hospital, connecting buildings and now its car parks. It has realised the cost benefits of using its existing advanced networking infrastructure rather than deploying dedicated coaxial cabling and is beginning to exploit these to the full.

As hospitals install more comprehensive networks and link via larger bandwidth lines onto Wide Area Networks (WANs) it will become possible for hospitals to share IP-based security resources using the services of a central monitoring station covering several hospitals. If one hospital can provide a monitoring centre for several this means that some will not have to devote resources to building and maintaining a security office with monitoring and control systems.