

installation of cctv systems
using IP technology
– a guide



May 2008

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Contents

1. Introduction	3
2. Scope	3
3. Definitions and abbreviations	3
4. Considerations	4
5. Network security	6
6. Network integrity	6
7. Management of the network	6
8. WAN Links	6
9. Customer IT departments	6
10. Maintenance	6
11. Training	7
12. Documentation and records	7
13. Reference documents	7

1. Introduction

The introduction of Internet Protocol (IP) based technology into the field of CCTV systems has created uncertainties which have inhibited the exploitation of the benefits available by adopting it. In particular, the growing use of Information Technology (IT) equipment and methodology to achieve CCTV functions requires that the CCTV installer be able to recognise the impact of using this type of equipment. A CCTV system operating over IP may require collaboration between the installer and IT specialists.

With the emergence of IP signalling technology, the benefits of remote CCTV monitoring are being realised as a cost effective and efficient alternative to conventional technology. Whilst references are made in this document to remote transmission capabilities of CCTV to Remote Video Response centres, it is not designed to cover all aspects of remote monitored CCTV systems as this is covered in BS8418 for detector-activated CCTV systems.

These guidelines have therefore been prepared to provide guidance on what a CCTV system will require from an IP perspective. It should be read in conjunction with the BSIA basic user, installer & ARC/ RVRC guides and other BSIA published documents from the IP suite.

2. Scope

These guidelines are designed to provide installers with an overview of the common considerations of systems combining CCTV functions within IP networks.

3. Terms, definitions and abbreviations

- 3.1 Bandwidth** – the amount of digital data transmitted between devices over the network. Usually expressed in bits per second (bps) i.e. Kilo (K)bps, Mega (M)bps.
- 3.2 CCTV system** – system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which might be necessary for the surveillance of a defined area of interest.
- 3.3 DVR** – A digital recorder for the recording of video from analogue signals; DVRs may be networked enabled such that they can be remotely accessed over an IP network.
- 3.4 Hosts** – Devices or appliances that make use of a network to send digital data.
- 3.5 Hybrid** – Common term used to describe a CCTV system or component making use of both IP and analogue parts.
- 3.6 IP** – Internet protocol - IP is an address of a computer or other network device on a network using IP or TCP/IP.
- 3.7 Infrastructure** – for the purposes of this document taken to mean the basic network construction for transmission of digital data e.g. predominantly the cables and switches used to send data from host to host.
- 3.8 IT** – Information technology - a broad term covering the various disciplines relating to communications and computer-based information systems.
- 3.9 LAN** – a physical network installed and managed entirely by the user.

Note: A LAN may include wireless connections.

- 3.10 Latency** – The time delay between the moment an event is initiated, and the moment one of its effects begins or becomes detectable (i.e. end-to-end delay).
- 3.11 Network** – Common term used to describe a ‘computer’ network whereby devices are able to transmit digital data to each other using common communication protocols
- 3.12 NVR** – A form of DVR that records video directly from IP video devices via network connection. This is the common term for recording devices used within IP-systems.
- 3.13 Switch** – networking device that connects computer devices together and passes data between them; a fundamental part of a LAN.
- 3.14 WAN** – a physical network of multiple LANs linked by a third party provider such as a Telecom.

4. Considerations

4.1.1 Operational Requirement

As a CCTV system, the first consideration should be the purpose of the system in terms of camera location, live viewing and recording requirements.

4.2 Bandwidth

IP-based systems are more likely to make more use of the network to transmit video data than a DVR-based system, especially if IP-cameras and video encoders are being used. Image resolution, compression level and frame rate will directly result in a bandwidth requirement from the network. A successful system will need to balance the bandwidth available against the minimum image quality requirements. Bandwidth requirements for the proposed system should be considered at the earliest opportunity to determine the viability and possible additional network requirements of an IP solution.

4.3. Latency

As the network utilisation increases, so does the potential for network latency (end-to-end delay) increase. The effects of latency on interactive functionality, such as Pan / Tilt / Zoom camera control and audio communication, should be considered at the design stage of the CCTV system.

4.4 Storage

The basic storage requirements will be the same for digital imagery irrespective of whether a DVR or NVR is used. Many NVR systems are able to make use of IT network storage systems that are independent of the NVR as well as to the hard disk drives located within the NVR itself. If networked storage is used then sufficient bandwidth between NVR and storage device must also be provided.

4.5 Compression effects on bandwidth and storage

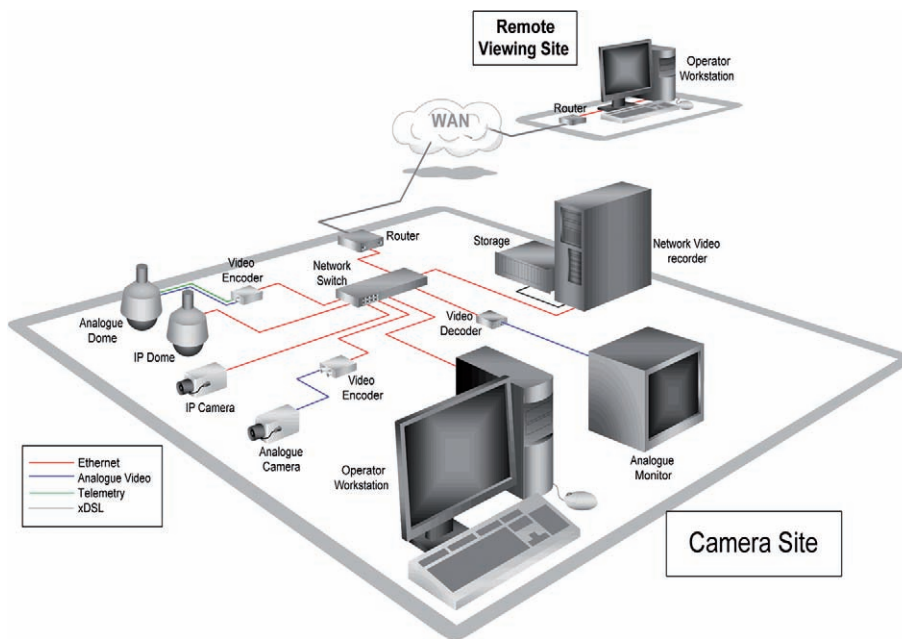
The way compression algorithms work can have a substantial effect on bandwidth and storage requirements. Conditional algorithms that enhance compression based on inter-image differences will generally produce digital image data that varies in size depending on the amount of activity in the field of view of the camera. When calculating bandwidth and storage requirements, this effect should be taken into account and the appropriate measures implemented.

4.6 NVRs

Whereas the maximum number of cameras a DVR can record will be limited by the number of BNC connectors it has, an NVR can technically connect to any number of network video devices. The limiting factor is therefore typically a factor of the NVR hardware's ability to throughput video data from the network through to storage system. This will depend on the bandwidth of the video stream from the video devices. The OR for recording should be used to establish how many cameras the NVR can practically support.

4.7 Network Design

The key to any IP system is the design of the network infrastructure that binds it all together. The following drawing shows a typical connection layout with the more common IP connective devices.



3.7.1 Network Topography

When the location of the various system components is known, the layout of the network can be evaluated and decisions made as to where any existing cabling can be used or where new cabling needs to be run. Standard twisted pair (CAT5) Network cabling does not run as far as co-axial video cable (usually limited to 100m or less) but there are many options to extend cable runs using standard IT methods and products.

3.7.2 Network usage

A key consideration for network video systems is the choice of using existing network infrastructure, enhancing the existing network or running an independent parallel network for the CCTV system. Only when the location of the equipment and the volume of data communicated between all devices is clearly understood can a clear choice can be made. There are many factors that affect this and most will be based on IT experience.

5. Network security

A risk assessment should be carried out to assess the possible vulnerabilities of a network installation. Appropriate actions should be taken to protect the network and hosts from physical and electronic attack, this should include stored or transmitted data.

Where Firewalls are used to protect the Network, a special configuration of the Firewall may be required to grant remote access to the CCTV system.

6. Network integrity

[Considered part of 'security' by IT] The design of the network should ensure not only a level of service suitable to the CCTV application but also a level of robustness (or availability) suitable to the CCTV system. This is also referred to as 'Quality of service' whereby a predetermined bandwidth and % availability will be specified.

Consideration should also be given to the concept of network available resources where additional capability is provided by a non-security source for the CCTV system. An example of this may be networked storage or operator workstations.

7. Management of the network

Networks may be considered more flexible than conventional CCTV systems in that they may use the same infrastructure for more than one purpose; the loading on that infrastructure may consequently be more variable. In systems where the service level (or quality of service for the CCTV function) is not guaranteed, consideration should be given to managing that network to monitor the performance and ensure corrective action where required. Where methods to control the network traffic are in use, an assessment should be made as to the impact of this on the CCTV system.

8. WAN links

Where CCTV data is to be sent via a WAN link, the appropriate link should be supplied. WAN links typically offer less bandwidth than LAN links and may be shared with other network functions. Careful planning is required to ensure optimal use of the link without degradation of other services.

9. Customer IT departments

CCTV installers should look to engage with existing IT departments at the earliest opportunity (preferably at system design stage) to ensure best practice and management of the system, particularly if an existing network is to be shared for the CCTV operation.

10. Maintenance

Maintenance or Service Level Agreements (SLAs) should be implemented according to requirement. IP CCTV systems will most likely be a hybrid of security and IT equipment and may therefore use different engineering resources for maintenance or repair.

11. Training

IP CCTV systems can offer new approaches to the provision of conventional CCTV functions and may therefore require additional training to familiarise engineers, administrators and users in the installation, configuration, usage and service of the system. The ability to understand basic IT skills and DOS commands will prove invaluable.

12. Documentation and records

The system design proposal and / or contract documentation should include the following information:

- Use of fixed IP addresses, either manually allocated or assigned by automated method (DHCP)
- User names and passwords
- Contact and policy details for the providers of the SLAs of all equipment
- Extent of maintenance coverage (who is responsible for what).

13. Reference documents

Standards publications

BS8418 Installation and remote monitoring of detector activated CCTV systems.

BS8495 Code of practice for digital CCTV recording systems for the purpose of image export to be used in evidence.

BSEN50132-7 CCTV Application guidelines.

Further reading

BSIA installation of IP based secure signalling systems for I&HAS

BSIA installation of access control systems using IP technology

BSIA ARC / RVRC guide to IP in the security industry

BSIA guide to common issues experience in Internet Protocol in the security Industry

BSIA installer guide to Internet Protocol in the security industry

BSIA User guide to Internet Protocol in the security industry

BSIA Form 120 Maintenance & servicing of CCTV systems

BSIA Form 109 Planning, installation and maintenance of CCTV systems

IPCRes guidance – Alarm signalling using Internet Protocol – Part 1 An overview

IPCRes guidance – Alarm signalling using Internet Protocol – Part 2 Considerations for insurers

HOSDB Operation Requirements manual Pub. 55/06