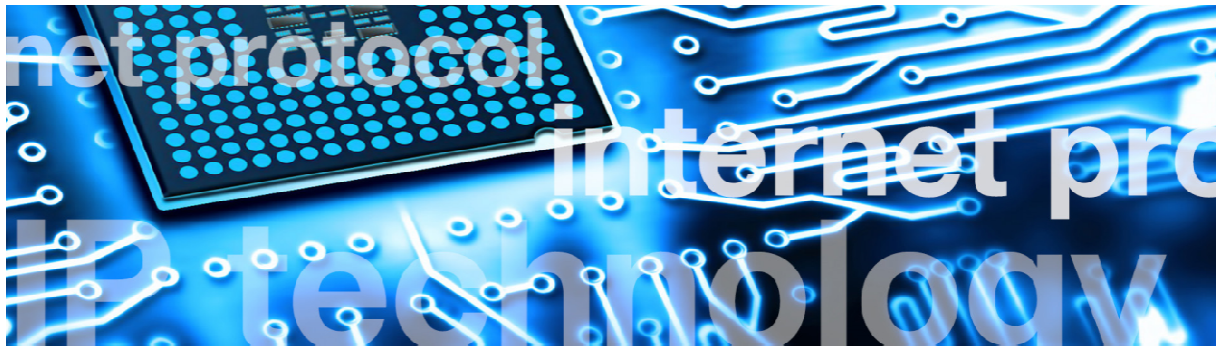

Installation of CCTV systems **using IP Technology** – a guide



September 2018

For other information please contact:

ODC t: 0845 389 3889
e: cctv@odc.vu
www.odc.vu

Contents

1. Introduction	2
2. Scope	3
3. Terms, definitions and abbreviations	3
4. Design Considerations	4
4.1. Operational Requirement (OR)	4
4.2. Bandwidth	4
4.3. Latency	4
4.4. Storage	4
4.5. Compression effects on bandwidth and storage	4
4.6. NVRs and Cloud Services	4
4.7. Network Design	5
4.8. Network Topography	5
4.9. Network usage	5
5. Network security	5
6. Network integrity	5
7. Management of the network	6
8. WAN links	6
9. Customer IT departments	6
10. Maintenance	6
11. Training	6
12. Documentation and records	6
13. Reference documents	7
13.1. Standards publications	7
13.2. Further reading	7

1. Introduction

The growing use of Information Technology (IT) equipment and methodology to exploit CCTV functions requires that the CCTV installer be able to recognise the impact of using this type of equipment. A CCTV system operating over Internet Protocol (IP) may require collaboration between the installer and other parties, such as 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 (RVRCs), it is not designed to cover all aspects of remotely monitored CCTV systems as this is covered in BS8418 for detector-activated remotely monitored 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 other BSIA published documents from the IP suite (see section 13, Reference documents).

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 that can be transmitted between devices over the network in a fixed amount of time. Usually expressed in bits per second (bps), i.e. Kilo (K)bps, Megabits (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 protected area.
- 3.3. **Cloud Services** – storing and accessing data and programs over the internet instead of local computers or local servers (hard drives).
- 3.4. **DVR** – A digital video recording device for the recording of video data; DVRs may be network enabled such that they can be remotely accessed over an IP network.
- 3.5. **Hosts** – Devices or appliances that make use of a network to send digital data.
- 3.6. **Hybrid** – Common term used to describe a CCTV system or component making use of both IP and analogue parts.
- 3.7. **IP** – Internet Protocol is the method or protocol by which data is sent from one computer (or other network device) to another on a network or the Internet.
- 3.8. **IP Address** – IP address of a computer or other network device on a network using IP or TCP/IP. Each computer (or other network device) on the network/internet has at least one IP address that uniquely identifies it from other computers or other network devices on the network/internet.
- 3.9. **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.
- 3.10. **IT** – Information Technology, a broad term covering the various disciplines relating to communications and computer-based information systems.
- 3.11. **LAN** – Local Area Network, a physical network sharing a common communications line or wireless link to a server covering a small geographical area e.g. office, school etc.
Note: A LAN may include wireless connections.
- 3.12. **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).
- 3.13. **Network** – Common term used to describe a ‘computer’ network whereby devices are able to transmit digital data to each other using common communication protocols (e.g. IP).
- 3.14. **NVR** – A form of DVR that records video data directly from IP video devices via network connection(s). This is the common term for recording devices used within IP-systems.
- 3.15. **Switch** – networking device that connects computer devices together and passes data between them; a fundamental part of a LAN.
- 3.16. **WAN** – Wide Area Network is a telecommunications and / or computer network that extends over a large geographical area.

4. Design Considerations

4.1. Operational Requirement (OR)

The OR is a formal document that outlines the CCTV system objectives, this should consider the threat assessment and risk analysis, and incorporate the customer needs. The CCTV system should be designed and installed in accordance with the requirements of BS EN 62676 series of standards.

CCTV equipment is available in grades therefore selection of security grades (dependant on threats and risks) is important. The location of equipment; how the system is to be managed and operated and monitoring / storage requirements should also be considered. For more information see British Standard BS EN 62676-4 Video surveillance systems for use in security applications – Application guidelines, and BSIA Form 218 Graded Requirements Under BS EN 62676 Standards for CCTV – a technical guide for installers and specifiers.

4.2. Bandwidth

IP systems are more likely to make 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 have a direct impact on the bandwidth requirement of the network. A successful system will need to balance the bandwidth available against the minimum image quality requirements of the OR. Bandwidth requirements for the proposed system should be considered at design stage to determine the viability and possible additional network requirements of an IP solution.

4.3. Latency

As the network utilisation increases, the potential for network latency also increases. The effects of latency on interactive functionality, such as camera control (e.g. pan/tilt/zoom) and audio communication, should be considered.

4.4. Storage

The basic data 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 an NVR. 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

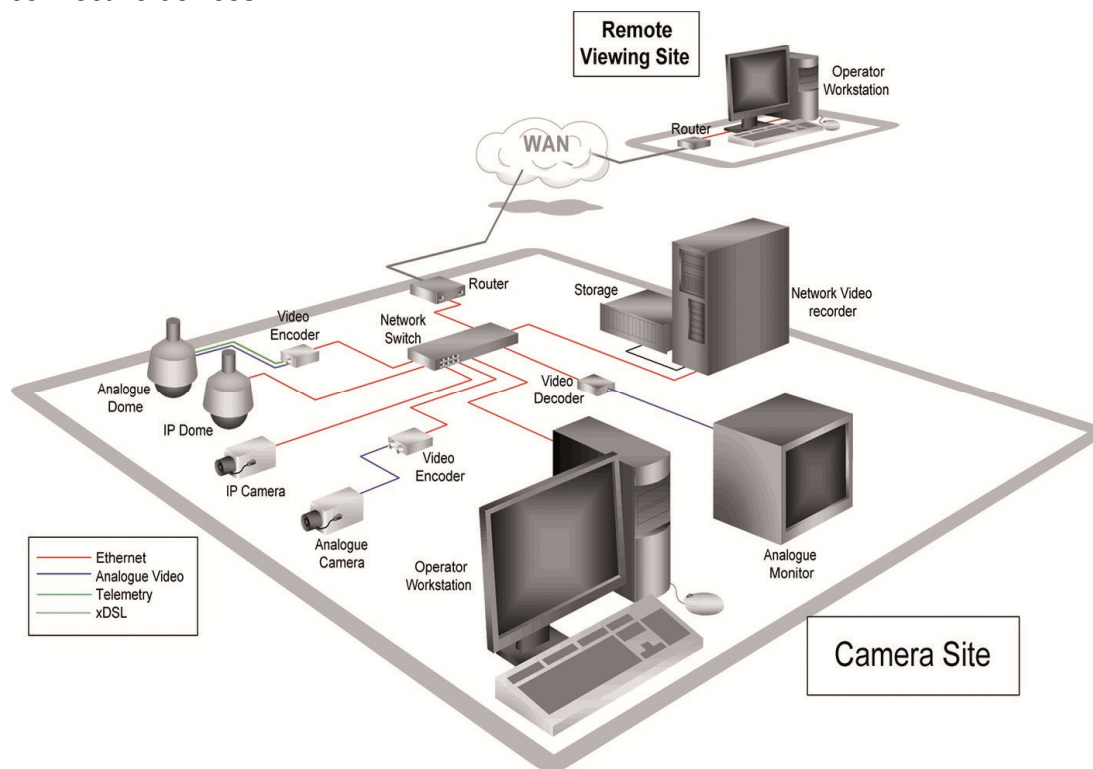
The way in which compression algorithms work can have a substantial effect on bandwidth and storage requirements. Conditional algorithms that enhance compression based on inter-image differences will generally produce digital image data that varies in size depending on the amount of activity in the field of view of the camera. When calculating bandwidth and storage requirements, this effect should be taken into account and action taken where necessary to ensure that the network can support this additional traffic.

4.6. NVRs and Cloud Services

Whereas the maximum number of cameras a DVR can record will be limited by the number of BNC connectors it has, an NVR or cloud services can technically connect to any number of network video devices. The hardware of the NVR or cloud services is typically the limiting factor based on its ability to throughput video data from the network through to the 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 or cloud services 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 drawing below shows a typical connection layout with some of the more common IP connective devices.



4.8. Network Topography

Once the location of the various system components has been determined, 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 installed. Twisted pair (CAT5, CAT5e or CAT6) UTP network cabling does not run as far as co-axial video cable (usually limited to 100m) but there are many options to extend cable runs beyond 100m using standard IT methods and products.

4.9. 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 specifically 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 be made. There are many factors that affect this and most will be based on IT network 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 the hosts connected on it 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 the IT industry] 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 (ideally in the OR).

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 that corrective action is taken 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 (and therefore security).

8. WAN links

Where CCTV data is to be sent via a WAN link (e.g. cloud services), 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 or security.

9. Customer IT departments

CCTV installers should seek engagement with existing IT departments at the earliest opportunity (preferably at system design stage) to ensure that there is co-operation and mutual understanding of the management and technical requirements of the system, particularly if an existing network is to be shared by the CCTV system.

10. Maintenance

Maintenance or Service Level Agreements (SLAs) should be applied according to the requirements. IP CCTV systems could 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 installers, administrators and users in the installation, configuration, usage and service of the system. The ability to understand basic IT skills will prove invaluable.

There are growing claims made by manufacturers as to the 'plug and play' capability of their equipment, however often to integrate this equipment into a system it requires access to advanced settings and in-depth knowledge of IP networks.

12. Documentation and records

The system design proposal and/or contract documentation should include (in addition to what would be required by a conventional CCTV system) 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

13.1. Standards publications

BS 8418 Installation and remote monitoring of detector-activated CCTV systems – Code of practice.

BS EN 62676-4 Video surveillance systems for use in security applications – Application guidelines.

13.2. Further reading

BSIA Form 109 – Code of Practice for the planning, design, installation and operation of CCTV systems

BSIA Form 120 – Maintenance of CCTV Surveillance Systems - Code of Practice

BSIA Form 210 – An installer's guide to Internet Protocol (IP) in the security industry

BSIA Form 211 – A user guide to the use of Internet Protocol (IP) in the security industry

BSIA Form 218 – Graded Requirements Under BS EN 62676 Standards for CCTV – a technical guide for installers and specifiers.

BSIA Form 234 – A Guide installation of IP based secure signalling systems for I&HAS

BSIA Form 235 – A guide for installation of CCTV systems using IP technology

BSIA Form 236 – A Guide to Internet Protocol for ARCs and RVRCs

BSIA Form 261 – Installation of access control systems using IP technology - a guide

BSIA Form 299 – Benefits of IP in CCTV

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

IPCRes guidance – Alarm signalling using Internet Protocol – Part 2 Considerations for insurers* **IPCRes guidance is published by the Fire Protection Association (FPA).*

Home Office Scientific Development Branch (HOSDB) – CCTV Operational Requirements Manual 2009 Publication No. 28/09

http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctvpublications/28_09_CCTV_OR_Manual2835.pdf?view=Binary

Surveillance Camera Commissioner's Surveillance Camera Code of Practice (SCCoP)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157901/code-of-practice.pdf

This document was created by the CCTV Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

CCTV has had a profound impact on crime prevention and detection. The UK leads the way in the application of CCTV and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition (ANPR) as well as many other functions.

In order to provide guidance and simplification in the complex area of CCTV, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The CCTV section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the police, inspectorates and insurers.

As a security company, BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

ODC Ltd

Unit 2 - TGE Building
Champagne Estate

Port Vila

VANUATU

t: +678 7728082

e: cctv@odc.vu

www.odc.vu

