bsia
british security industry association

an installer's guide to **internet protocol (IP)** in the security industry

June 2007

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

Form No. 210

Contents

1. Introduction

The use of Internet Protocol (IP) in security applications has become increasingly commonplace and the new generation of 'digital' systems is seeing a trend towards IP in all applications. Traditionally this has been a predominantly Information Technology (IT) dominated area, but security installers are now being asked to provide IP solutions which require an understanding of IT.

This guide is aimed at providing installers with a basic understanding of the concepts of IP in security applications and to assist in the design and installation considerations. It forms part of a suite of documents produced to aid end-users, IT managers and installers at both a basic and a more technical level.

2. Document references

a. Information references

The following referenced documents complement this guide:

There are several documents in the process of development which include:

- BSIA Basic User guide to the use of Internet Protocol in the Security Industry
- BSIA Guide to Installation of CCTV Systems Using IP Technology
- BSIA Guide to Installation of Access Control Systems Using IP Technology
- BSIA Guide to IP Systems Monitored by ARCs/RVRCs
- BSIA Code of Practice for the Installation of IP based Secure Signalling Systems for I&HAS

Please check the BSIA website for latest information.

b. Bibliography

- IPCRes guidance: Alarm signalling using the Internet Protocol – Part 1: An overview
- IPCRes guidance: Alarm signalling using the Internet Protocol – Part 2: Consideration for Insurers
- prEN50136-1-5 Alarm systems – Alarm Transmission Systems and Equipment: Packet Switched Network

3. What is IP?

IP is part of the 'Internet Protocol Suite' which includes a number of different protocols for the delivery of data over a network. IP addressing is part of this protocol suite.

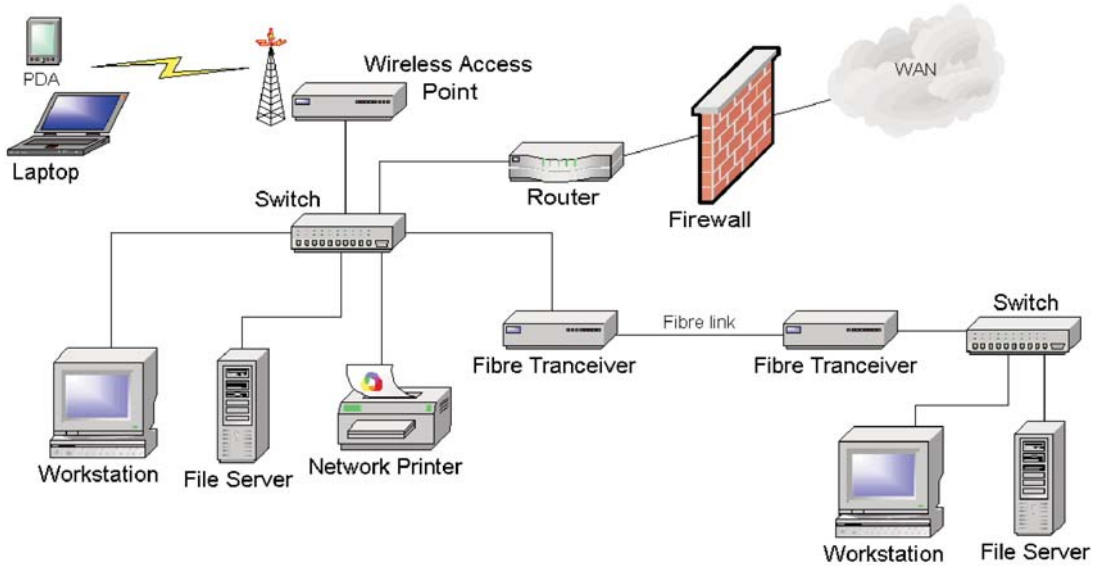
TCP/IP and UDP/IP are the most common protocols used in conjunction with IP addressing; UDP is one of the main protocols used for the management of the 'internet' and is becoming more common for security applications.

Although UDP in its basic form has no confirmation of delivery (whereas TCP includes "reliable" delivery of data), an acknowledgment protocol can be added to provide this.

4. What is a network?

A network is a group of connected communicating devices such as computers, printers, CCTV and access control equipment. The rationale for a network is that it makes possible the sharing of resources and the provision of access to remote information and person-to-person communication.

The connection between the equipment need not be copper wire. Fibre optics, microwaves and satellites can be used.



a. What is a LAN (Local Area Network)?

The term LAN refers to a group of connected devices in a home or office. Ethernet is the most widely used LAN protocol. The data transmission speed is normally up to 10/100 Mbps (10/100 million bits per second), and 1000Mbps are available.

Note: Know your Bits from your Bytes

It is important to understand the relationship between the measurements of 'bits' & 'bytes' as this impacts greatly on specification of networks and components. A 'bit' is a nought or one. A 'byte' is eight bits. Once you understand this, all other measurements are just a multiple. Storage volumes are usually stated in bytes and communication capacities (transmission capacity is called bandwidth) are stated in bits, usually bits per second (bps). This is how you can get caught out because a transmission capacity of 32 Kilobits per second is only 4 Kilobytes per second, so as a rule transmission speed is defined in Bits and storage is defined in Bytes. Common terminology is usually Kbps or Mbps. You always need to understand whether you are talking BITS or BYTES!

The two vital components to connect a LAN together are Network Interface cards (NICS) and cables. Each hardware device on the network must have a NIC, and a network cable connecting it to the network. Some devices such as PCs, DVRs and Alarm panels have NICs built in.

The NIC has a unique address to identify itself; this is called the MAC Address (Media Access Component Address). The MAC is a 6-byte physical address that is unique to every NIC. Each byte in the MAC is separated by a dash. For example 44-45-53-54-42-00.

b. What is a WAN (Wide Area Network)?

A WAN is the means in which LANs can be connected together. A WAN covers a broader geographical area than a LAN. The largest and most commonly used WAN is the Internet.

c. What is an IP address?

In order to pass information between network-attached devices (hosts) each NIC in an IP network requires an IP address. IP addresses are a simple way of associating a MAC address with a logical network address and are unique within each network. An IP address can be static or dynamic (refer to section D).

Additionally, every IP address will be associated with a subnet mask. A subnet is a division of an IP network. The subnet mask is used to identify the size of a network segment and the number of hosts supported in it.

If a host needs to share information beyond the local area network, it must be configured with a gateway address. A gateway is a host on the network that connects to other networks, e.g. a router or firewall. The gateway is responsible for routing information between networks.

For every host (CCTV, intruder alarm, access control) that needs to be accessed remotely or send information, an IP Address & Subnet Mask is required. If information is to be shared between two networks (security system & ARC/RVRC) a gateway address is also required.

Small networks will typically use an address that looks something like 192.168.0.1. This network could in theory provide up to 65535 network addresses that cannot be directly accessed from the Internet. In practice it is more likely that the network will be limited to 255 addresses or less.

There are two types of IP address:

- Public: The IP addresses are accessible via a WAN, (e.g. the internet). This means communication to a security system with a public address can be accessed from any point on the WAN (internet).
- Private: A private address is one that cannot be directly accessed from a public network, i.e. from the Internet. There are three ranges of addresses that have been reserved for private networks and will never be used on the Internet. For this reason, they are the most popular address ranges used on private networks. An internationally approved document sets this out in more detail (http://rfc.net/rfc1918.html).

Private address ranges available are:
192.168.0.1 – 192.168.255.254, 172.16.0.1 – 172.31.255.254 & 10.0.0.1 – 10.255.255.254

d. How do you assign IP addresses to a device?

For a security system providing no integral method, it is likely that configuration of an IP address will be achieved using a directly attached RS232 link, a web browser, software utility and/or a telnet session from a PC or other similar device.

Before you can assign an address, you will need to know if a static or dynamic address is to be used. This can be determined from the manufacturer's information and what has been agreed with the customer.

- Static addresses: A static address is permanently assigned to the network host.
- Dynamic Address: In a network that provides dynamic network addressing, a pool of reserved addresses is allocated to a service called DHCP (Dynamic Host Control Protocol). DHCP is listening out for address requests. As a device such as a laptop connects to the network, it broadcasts a request for an IP address, i.e. an association with its MAC address. An IP address is returned with some other essential information,

e.g. subnet mask, gateway address, DNS details, etc. The address is leased to the laptop for a preset length of time. In this way, the laptop user does not need to know the network-addressing scheme. When the lease expires, the IP address is returned to the DHCP pool. Consequently, a network is less likely to run out of addresses and the need for manual records of assigned addresses is greatly reduced.

- It is possible to have both options used on the same network, e.g. on a network limited to 254 addresses, 50 IP addresses could be allocated to the DHCP service leaving 199 possible static IP addresses.

As it is likely that an IP enabled CCTV system has been installed to provide remote viewing, it is unlikely that dynamic addressing will be used. The reason for this is that the system's address will have to be known on the network in order to provide remote access. i.e. if you don't know the address, you won't be able to view the images.

However, for systems that only send information to another network host (ARC/RVRC) the IP addressing could be either static or dynamic.

Annex B & C provide useful guidance on simple tests and DOS commands used for testing and identifying issues with IP based systems.

5. Types of transmission media

A network is a group of connected communicating devices such as computers, printers, CCTV and access control equipment. The rationale for a network is that it makes possible the sharing of resources and the provision of access to remote information and person-to-person communication.

a. Cable connectivity – There are three main types of network cables used:

- Unshielded Twisted Pair (UTP) such as CAT5 & CAT 6
- Coaxial Cable
- Fibre Optic Cable

UTP cable typically provides for cables runs up to 100m when used with Ethernet. It is important to use the correct grade of UTP, i.e. CAT 5 for 100Mbps and CAT 6 for 1Gbps. This type of cable is very cheap to purchase and is flexible and easy to install. It is also used by other networking systems than Ethernet and may for instance be used to provide telephone lines to offices. The commonality of UTP cabling, which is used for many purposes, eases installation and management of the cabling.

Fibre-optic cable provides the highest speed and greatest capacity for transmission of data, up to 40Gbps. It is becoming more cost effective to install. There are two main types of fibre 'multi-mode' which is cheaper, has less bandwidth capability and shorter range, and 'single-mode' which is more expensive, has more bandwidth capacity and operates over longer distances.

b. Wireless connectivity

There are a number of different methods that can be used to send network data over wireless links. Typical solutions will use either radio, microwave, laser or GPRS technologies.

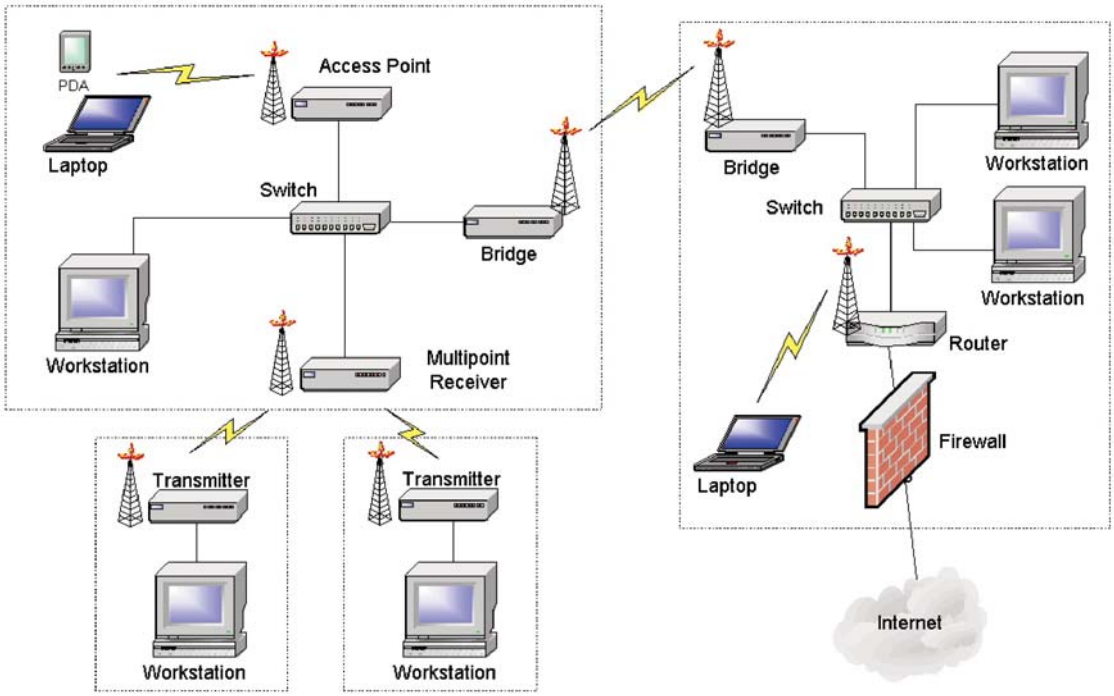
Which type of wireless connection to use depends on environmental conditions, the availability of such services and whether the link provides sufficient bandwidth for the security application.

Wireless connections operate in a number of different ways.

- Point–to-point links are the most basic connections where the wireless link effectively substitutes for a cable. This is sometimes referred to as a wireless bridge.
- Point-to-multipoint links operate on a similar principle, but have multiple single links connecting to a single central receiver. Access points (Wi-Fi) are a form of this.
- Mesh networks use multiple single and multi-point links to link together many transmitters/receivers across diverse environments with multiple connection paths between them.

Wireless systems are a mix of standardised (usually to IEEE standards) and proprietary technologies.

The most common form of wireless use in IP networking is to extend a LAN over wireless links, referred to as Wireless LAN (WLAN).



6. Types of hardware

The types of hardware that form a network are vast and varied. There is a great deal of choice in both quality and functionality. Some examples of typical network hardware are listed below.

A typical LAN will consist of hosts (PCs, servers, security systems), hubs/switches and various cabling and interconnections. If the LAN is connected to another network, e.g. the Internet, a router will also be present.

a. Hubs & Switches

All the hosts on a LAN are connected together using cables connected to a hub or a switch.

A hub has the poorest performance since it has no built-in intelligence. A hub literally sends network traffic from any one device to all devices connected to it. This creates network performance issues and would definitely not be recommended for CCTV applications.

A switch, on the other hand, does have some intelligence built in. It quickly builds a list of hosts attached to each port and only forwards traffic between the two hosts as required. In this way it avoids the performance problems of a hub.

b. Networking issues

The Internet does not have an infinite number of addresses available. This is one reason why the use of private network addresses is so common.

However, for any network connection to the Internet, a public address must be used. It is very common practice to hide a LAN consisting of many hosts behind one public IP address. In this way, hosts on the LAN can send traffic across the Internet; web browsing, email, etc.

To send information to a host on the LAN from a remote location, the LAN must have a public IP address and a method of identifying one of the many hosts behind the public IP address. This is done using Network Address Translation and Port Forwarding.

c. Firewalls

A firewall is a software or hardware system which limits network access between two or more networks. Normally, a Firewall is deployed between a trusted, protected private network and an un-trusted public network. For example, the trusted network might be a corporate LAN and the public network might be the Internet.

Consider a private corporate network consisting of various PCs and servers. There is no requirement for any of the PCs and servers to be directly accessed from the Internet. However, there may be a web server that allows Internet users to view information provided by the company.

Clearly, the company wants people to view their website but not the contents of the accounts server on the LAN. However they are likely to want users in the LAN to view other Internet pages and have access to email, etc.

For a security system connected to an ARC/RVRC across the Internet, a router and firewall arrangement will be used. It is quite common for these to be combined in the same unit.

d. ADSL Modem

Most ADSL modems have an integral firewall and are a convenient way of connecting a LAN or host to the Internet. If the ADSL modem is going to be used for security systems, it should have appropriate network connections. Some are limited to USB connection to a PC only.

e. Network Address Translation (NAT)

A host on a LAN can access the Internet without the need for a dedicated public IP address

NAT modifies outgoing network requests so that the return address is a valid public IP address (i.e. the address assigned by the internet service provider). Return (incoming) responses have their destination IP address changed back, and are relayed to the host. This protects the private IP addresses from public view.

f. Ports & Port forwarding

You could think of an IP connection like a large pipe. At the end of the pipe you have a grid with 65535 holes or ports.

Some of the ports are reserved for applications like email, web hosting, telnet, ftp, etc. , but the vast majority of ports are not reserved and can be used by any application. For every connection to the Internet one of these ports is used.

Where public access to a host on a LAN is required, it is possible to reserve one of the ports and associate it with an application running on one of the LAN hosts with the use of a firewall.

Example of multiple hosts accessed using a single IP address:

The public IP address of the LAN = 123.123.123.254

Private IP address of customers web server = 192.168.1.1
Port number of web server = 80
Private IP address of the first CCTV system = 192.168.1.2
Port number of web server embedded in the first CCTV system = 80
Private IP address of the second CCTV system = 192.168.1.3
Port number of web server embedded in the second CCTV system = 80

Port forwarding rules could be set up so that any traffic destined to:

123.123.123.254 port 80 = 192.168.1.1 port 80
123.123.123.254 port 8080 = 192.168.1.2 port 80
123.123.123.254 port 8081 = 192.168.1.3 port 80

In a web browser you might type: http://123.123.123.254:8080 to get to the first CCTV system

Although it is possible to route IP traffic between a LAN and an ARC/RVRC via the Internet using only a router, it is not likely. This is because a router without a firewall is not very good at filtering traffic from authorized/unauthorized access to hosts on the LAN.

Remote access to LANs (particularly via the Internet) brings its own challenges and introduces the concepts of 'fire-walling' for security and "port forwarding" when initiating a connection to a device on the LAN from outside. Support for network configuration should be confirmed before attempting to carry out any external access to the LAN.

A router should be considered in a private network only where all hosts on the network are trusted.

7. Specifying an IP application

As with all technology, IP requires careful consideration. Good system design and communication between interested parties such as installer, client and IT manager/provider are vital BEFORE any installation is commenced.

The design of the network must ensure continual operation in order that the security system can function correctly. Note for 'internet' networks there is no guarantee that the message will be delivered. For business LANs, there is always the possibility of down time from either system maintenance or malicious attacks. To overcome these issues a redundant path (e.g. POTS, ISDN, GSM) should be considered. This would be enabled when there are network problems.

It is important to decide/agree whether the security application will use the existing network or be for the sole use of the application; where the existing network is used, this will require careful planning to agree a network design to accommodate both client and security needs.

Different security applications require different considerations. For example, a CCTV system (or integrated system incorporating CCTV) would need to consider greater bandwidth requirements due to the constant stream of large amounts of video data (this is covered in more detail in Section 8 'Bandwidth').

Integration of security and/or safety applications is becoming more commonplace (See BSIA Guide for Integrated Security Management Systems) and again is a major consideration as it can bring together different technologies into a single management system, improve audit trails, increase operational efficiency and provide cost savings.

If there is a requirement to send IP data from the network (LAN) to a remote location (use of a WAN), and conversely there may be a need to access the security system remotely, then consideration must be given to the use of Firewalls that protect information entering the local network.

The key elements associated with IP are covered in the various sections of this document and Annex A provides detail of the more common issues and considerations associated with IP in security applications.

8. Integrating analogue with IP

IP networks offer the potential to transmit any form of information over a single connection type. To do this, the information has to be converted to a suitable digital format. Security devices that are based on analogue or non-network digital data formats (such as serial data) can be adapted to use network transmission through the use of transceivers, encoders or even PCs. These will sit in line between the security device and the network and have two interfaces, one appropriate for each side. Examples of such devices include:

- Serial transceivers that convert RS232/485 to a Ethernet
- Video encoders that convert composite video to Ethernet
- Network accessible DVRs that have composite video inputs
- Network modules that connect alarm panels to Ethernet
- Network Control Units connecting multiple access control devices to the network
- PCs that connect to serial LCUs and are network accessible

9. Bandwidth

Network bandwidth is a measure of how much data a communications channel can transmit every second, typically about 100Mbps. The bandwidth required depends not only on the compression method (see below), but also on the application.

Bandwidth is of particular concern for video applications for two key reasons. Firstly, video transmission is 'hungry' for bandwidth and secondly, it is sustained in requiring this hunger (whereas other applications such as access and intruder systems require less bandwidth and only uses it for small amounts of time).

Each IP system (digital video in particular) needs to be carefully sized for bandwidth at design stage, ensuring the existing LAN/WLAN can handle the additional data.

10. Compression

Digital video (and, to an extent, audio) creates very large volumes of data relative to the bandwidth available for its transmission and the storage available on which it can be recorded. Therefore, from a practical and cost perspective, some form of compression must be used.

When creating digital data, it is possible to compress the data to an extent without any discernable loss in content or quality. This is referred to a lossless compression, but this is not usually sufficient to meet the practical or cost limitations.

Most video applications will use 'lossy' compression methods to deliver an acceptable solution. These compression methods will use a number of methods to achieve this compression including:

- Discarding elements of video or audio that are barely discernable by the human eye or ear i.e. removing very high or very low audio frequencies or removing subtle colour shades or very fine detail in images.
- Using mathematical algorithms to find repeating patterns in digital data and hence removes repetition.
- Using a comparative process between previous and current data and only recording the differences i.e. only record the differences between one image and the next.

The net result is that the digital data will not be of the exact quality as the source. However, compression should not prevent the output of the system from providing information to adequately meet the purpose of the system.

11. Security considerations

This can be divided into two key areas, network and physical security.

a. Network Security

It is essential that consideration is given to the protection and security of information, both existing customer data and data associated with a security system.

This can be done in a number of ways, but in the case of security systems it is likely to take one of two forms: encryption or network security. Many security systems already have encryption built in. Where this is the case, decryption is completed between the various networked components of the security system. However, it may be the case that a security system does not have any in built encryption e.g. a CCTV web server may honour a request from any browser. In the case that external access is planned to such a device, it may not be appropriate to allow any web browser to connect. To protect such devices from unauthorised access, a simple approach might be to configure a firewall to accept connections from a few specific IP addresses. However, this may not be possible if static IP addresses are not available. The option you might choose as an alternative is to create a VPN tunnel between the CCTV web server and a web browser either by software or firewall configurations.

Some IT departments may require complex configurations to address security concerns.

Any firewall protecting the LAN from the Internet may have to be configured to allow information to be sent from the security system to a remote network. This is likely to be the case when dealing with larger corporate networks. If the security system is to be accessed from outside the LAN, i.e. the ARC/RVRC, then this brings its own concerns. Firstly, the LAN will have to be associated with at least one public IP address. A firewall will have to be configured to allow information to be sent to the security system but not expose any other host on the network to the WAN e.g. a customer's accounts information held on a

server on the same LAN. Consideration must be given to who will be responsible for configuring the external access.

For some security applications, consideration should be given to setting up user rights and creating a separate area on the network for different departments i.e. HR, finance, managers etc. The computer may be 'locked down' more than other computers on the network.

It is worth noting that some security systems will require a secondary signalling path to satisfy the needs of security and other key stakeholders such as insurers.

b. Physical Security

Physical access to the network components, e.g. unsecured workstations, power supplies, routers, firewalls etc and tampering with interconnections will need to be considered.

Note: Some security applications have industry agreements and/or standards that require certain conditions to be met to achieve the desired level of security. These are referenced in the bibliography and reference sections of this document.

Detailed consultation should be carried out with the client's IT Manager or network administrator to ascertain their requirements, in order to design the system effectively.

See Annex A for further guidance on considerations when specifying an IP system.

9. Acknowledgements

The BSIA would like to thank the IP Working Group for its contribution in the production of this guide.

Annex A

Considerations required when specifying a system

General

Does the client want to run the security application over the existing network?
How much bandwidth does the security application nominally use, will this affect other existing services?
How many IP addresses will be used and are static/dynamic IP addresses required?
Is the network secure, does it have external access (WAN)?
If using a WAN, check with the IT department that the ports used by the security application are enabled.
Does the network connection to the security application need monitoring, and, how often - every minute, every hour?
To improve security, consider limiting access to certain IP addresses. How many sites are there within the network?

The client may have to consider changes to their network to accommodate all the proposed devices e.g. extend a DHCP pool or address network security concerns.

If digital video, how many cameras are there to be:

a) recorded on each site
b) monitored remotely from each site (simultaneously)
a) how many viewing stations are required to view the cameras both locally and/or remotely?

How many images are to be viewed and transferred from the central control station for viewing by external organisations?

Video requirements

What IP compression technology is to be used e.g. must a lossless compression standard be used?

What are the images to be used for?

a) monitoring
b) surveillance
c) identification

What frames per second are required for:

a) live view of images
b) recorded images?

What resolution is required for each camera image?

a) live video
b) recorded video
c) remote transmission

Are the cameras PTZ or static or both and in which percentage?

IP transmission introduces delays at each stage, called 'latency; which is very minimal with good design but can be significant over remote access. A consideration when designing for real-time systems is the delay between viewing an image and a response to it e.g. if an operator is using a PTZ system to track a fast-moving object, the system should be designed to accommodate this need.

Audio

Is audio required (live, recorded or both)?

Alarms

Are there alarm inputs required? If so, consider increased resolution and/or frame-rate, alarm messaging etc?
Do relay outputs need to be driven?
Motion detection required?

If speed is paramount – consider using UDP as transmission format and ensure that the security product uses separate ports for alarm transmission and remote programming.

Data transmission

Is there an existing cabling infrastructure in place, or do new network cables need installing?
Is a wireless LAN being used, consider security of data?
Is data transmission required from multiple sites?

Recording

Does the video have to be recorded:

a) on site
b) within monitoring centre
c at any remote and or external viewing points
d) in more than one location simultaneously?

Is recording continuous, time scheduled, alarm/motion driven?

How many users will require to view recorded images from:

a) on site recordings
b) at a monitoring centre

For how long should recordings be kept?

a) on site
b) at a monitoring centre

What mediums are to support video storage? i.e. hard disc, CD, DVD, Raid, NAS

Network

Are the site devices to be capable of Simple Network Management Protocol (SNMP) for diagnostic purposes?
Are there to be any Network Address Translation (NAT) between transmitters and receivers?
Will the WAN link be private or public? If public (shared), what guaranteed bandwidth will be available?
Will the network (LAN / WAN) support Multicast - Internet Group Management Protocol traffic?
Is a redundant back-up transmission medium such as ISDN-2 required within each site?
Consider encryption when using Public Networks – if encryption is not available, check if VPN can be used instead.

Personal Computer (PC)

Things that need to be taken into consideration when using a PC:

a) processing speed
b) storage size
c) picture quality – number of Kbytes
d) picture format – CIF, 2CIF, 4CIF
e) bandwidth at different points on the network
f) type of motion – business of scene

Software

Is there multi-site control and management control of cameras via PC and keyboard, user password and access control, database of events, preset and tour camera functions, alarm.

Are all images downloaded to storage medium(s), watermarked, encrypted and date and time stamped for evidential purposes?

Redundancy

a) Network – recommend the usage of protocol such as spanning tree for multiple redundant path.
b) Storage – recommend the usage of RAID array systems i.e. RAID5 for video footage resilience or mirror recordings via network video recorder.
c) Network video recorder/PC – recommend internal dual power supply within equipment and or UPS back-up.
d) Suggest requirement back–up transmission medium such as ISDN-2 line per site.
e) System software and equipment to be capable of supporting multiple control stations to provide full disaster recovery facilities in the event of main control centre failure.
f) Are the multiple viewing stations server based i.e. one point of failure?

Annex B

Useful DOS commands (examples given below)

ping <IP address or host name>	Used to check interface between network devices e.g. ping 192.168.1.1
IPconfig	Display the IP address, mask, and default gateway for NIC.
IPconfig /all	Lists additional information such as the MAC address, and IP addresses.
arp –a	Display the logical IP address assigned, alongside the physical MAC address.
arp –s <IP address> <MAC>	Add a permanent static IP address to the MAC.
arp –d <IP address>	Delete the assigned static IP address.
traceroute <IP address>	List the network path taken to reach the IP address.
route add <destination IP address> <mask> <route IP address>	Any data destined for the destination IP address will be routed through the route IP address.
netstat <-s or –e or –r or –a>	Displays network statistics.
nbstat	Display NetBIOS table.

Free sniffer tools on the internet (for monitoring of network communication)

Ethereal	http://www.ethereal.com/
IP Analyzer	http://analyzer.polito.it/

Annex C

Tips for testing networks

1. **Testing ethernet products:**
   There is no need to use hubs or switches when testing the operation of an OEM product on a PC. By simply reversing the RX, TX connection of the ethernet cable, the product can be connected directly to the PCs ethernet port.

2. **Testing network applications on the same PC**
   The IP address 127.0.0.1 is used to direct data to applications that are internal to the PC. By using this address in your network applications, it may be possible to test two network applications on the same PC, thereby eliminating the need to use an ethernet connection.

3. **Network problems**
   Try pinging the device. This will not only inform you whether there is a connection from the PC to the device, but it will also inform you of the time taken to transmit the ping message.
   If a WAN is used, try using the traceroute command to determine location of problem, as this command will list all the network points that have been successfully negotiated.

   Use a free sniffer application such as ethereal to view the network activity on the LAN.

   Check that there is no duplication of IP address on the WAN.

Annex D
Terms & definitions

ADSL
Asynchronous Digital Subscriber Line.

Algorithm
Set of well-defined instructions that perform a certain task, for example a compression algorithm.

ARC
Alarm Receiving Centre.

Bandwidth
In networking terms, the capacity of a transmission channel to send digital data.

Bit/Byte
Basic structure of digital data, A bit is a single binary value. A byte comprises 8 bits. Most significant in that bits are used as the metric for transmission, bytes are the metric for data storage. Multiples of bps include Kilobits (Kbps), Megabits (Mbps) and Gigabits (Gbps).

Broadband
In networking terms, Broadband refers to communication using wider frequencies to provide higher bandwidth connections for WAN links.

CAT 5/6
Category of UTP cabling recommended for use for Ethernet networks. CAT5 is for 100Mb transmission, CAT6 for 1Gb.

CIF/2CIF/4CIF – Common Intermediate Format
A standard format for digital image resolutions based on a single CIF resolution image of 352 x 288 pixels.

CD – Compact Disc
A Compact Disc or CD is an optical discussed to store digital data.

Compression
In terms of networking, compression is the use of compression algorithms to reduce digital data in size to reduce the storage or bandwidth required to hold or send the data.

DHCP (Server) – Dynamic Host Control Protocol
Protocol that automates the assignment of IP addresses, subnet masks and other IP parameters. Usually implemented through a DHCP service running on a server.

Device
In simple networking terms, a device is something that performs a specific function on the network that is not a computer. Devices are very similar in concept to appliances and include switches, routers and video servers.

DNS
Domain name server.

DVD – Digital Versatile Disc
DVD also known as "Digital Versatile Disc" is an optical disc storage media format that can be used for data storage.

DVR – Digital Video Recorder
System that is capable of recording, playback and export of digital images captured by CCTV cameras.

Dynamic address allocation
The process by which a host is given an IP address by DHCP.

Encryption
The coding, translation or other modification of information, where the manner in which the information is modified, varies with time in a random manner.

Ethernet
Ethernet is the term for networking technologies standardised under IEEE803.2. Most commonly realised using UTP cabling but can also run over fibre.

Firewall
Security device designed to block unauthorised communications. Blocking is based on a set of rules that are based around IP and port address details of incoming (and outgoing) communications but do not examine the contents. Firewall will therefore not necessarily stop attacks such as viruses, which are attached to legitimate communications.

Gateway
Gateways can have different meaning within networking, but for the purposes of simple IP usage, the gateway is the IP address of the device that links to other subnets/networks. The best example of a gateway is a router.

GPRS – General Packet Radio Service
A mobile data service designed to increase speeds of transmission across a network.

GSM – Global System for Mobile communications
Digital cellular communication system used predominantly for mobile phones.

IEEE
Institute of Electrical and Electronics Engineers.

Internet
Global public network accessed through Internet Service Providers (ISPs) running on network infrastructure provided by many telecoms companies. Best known example of a WAN.

IP Address
An address format that hosts use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard.

IP address allocation
Assigning a specific IP address to a particular host or device.

IP – Internet protocol
A data-oriented protocol used for communicating data across a packet-switched network. IP operates over diverse networks.

IT – Information Technology
Broad term covering the various disciplines relating to communications and computer-based information systems.

Latency
In networking, the time delay in sending data and when it is received at its destination.

LAN – Local Area Network
A data network over which hosts 'local' to each other can communicate with each other. Typically considered to be limited geographically to within a building or group of buildings, ultimately a LAN can be considered to be constrained by its implementation, operation and management by a single organisation.

Lossless compression
Method of compression whereby all pre-compression data is kept during the compression process.

Lossy compression
Compression technique in which part of the original data is irretrievably lost.

MAC – Media Access Control
Unique address given to every Ethernet device programmed into the device at the time of manufacture. MAC addresses are managed by the IEEE and are globally unique irrespective of network usage, they cannot be changed.

Mirror recording
A form of redundant data recording whereby all data written to one disk drive is duplicated exactly on a second disc drive. Commonly implemented as RAID 1.

Mono - (single) - mode
Used to define a type of fibre-based transmission providing a high bandwidth over a long distance when compared to other equivalent transmission types.

Multicast
A more efficient method of transmitting information to a group of recipients using a centralised node system to redistribute data to local users instead of using many point-to-point links.

Multi-mode
Used to define a type of fibre-based transmission providing high bandwidth over a shorter distance when compared to mono-mode.

NAT – Network Address Translation
Redirects traffic for one IP address to another IP address by changing the destination IP address in transmitted data packets. Typically used by routers in conjunction with port forwarding when connecting LANs to a WAN.

Network availability
A measure of the amount of time the network is in a functional condition.

NIC- Network Interface Card
Component fitted to a computer or device that enables network connectivity. NICs can be bought as plug-in cards or more typically are now integrated within the computer/device hardware.

Network/System administrator
Individuals responsible for the configuration, maintenance and operation of a network.

OEM – Original Equipment Manufacturer
Company purchasing a manufactured product from another company and reselling the product under its own name and branding.

PC – Personal Computer
Relatively cheap computer designed for use by a single person.

Point-to-point
The most basic of network connections providing a single link between two hosts or devices.

Point-to-multipoint
Simple form of network where a number of hosts or devices connect to a single recipient host or device.

Port
A numeric suffix for IP addresses that identify specific software applications on a host to receive the transmitted information. Port numbers can be used freely but port 1024 and lower are reserved for certain applications, for example port 80 is used for web servers.

Port forwarding
Commonly used to describe the process whereby communications sent to a public IP address of a router attached to a WAN are redirected by the router to private IP address of a particular host on the LAN (see also NAT).

POTS
Plain Old Telephone System – also PSTN – Public Switched Telephone Network.

Private IP address
IP address of a host not directly connected to the Internet. Private IP addresses can be any valid address though there are conventions for the use of particular reserved IP address ranges to avoid inadvertent conflict with public IP addresses. Such ranges include 10.xxx.yyy.zzz and 192.168.xxx.yyy.

PTZ
Pan tilt and zoom.
Refers to capability of camera.

Public IP address
IP address used by a host connected directly to the Internet, typically assigned by an ISP. Public addresses are managed by regional Internet authorities to ensure unique usage.

RAID (array, 5) – Redundant Array of (Independent) Inexpensive Discs
RAID is a term describing data storage schemes that divide and/or replicate data among multiple hard drives. RAID 5 is a particular common form used in digital video recording of CCTV which provides a storage system capable of continued operation when one of the drives in RAID array fails.

Remote access
Can have several meanings in networking, but most commonly it refers to the accessing of local network resources from a remote location i.e. over a WAN. Is also used where resources normally accessed on a host directly are actually accessed from another host on the same LAN i.e. remote DVR clients.

Router
Inter-networking device that forwards data based on IP addressing usually linking LAN networks together.

RVRC
Remote Video Receiving Centre.

Server
A computer or device connected to a network that manages network resources. Examples include file servers, web servers, video servers and print servers. Servers typically run software services to achieve their functions. Some types of server can provide multiple services.

SNMP – Simple Network Management Protocol
Protocol comprising a set of standards for the remote monitoring of the state of operation of hosts and devices connected to a network.

Static IP address
An IP address that is allocated to a specific host and does not change automatically.

Subnet mask
'Subnetting' is the division of IP address ranges into smaller subordinate networks (ergo "subnet") for allocation of addresses to different organisations and the management of hosts and communications. The subnet mask is a value used logically by hosts to determine if the destination IP address in the same subnet as the host.

Switch
Networking device that transparently connects hosts or devices to each other as a LAN.

Transceiver
A device containing both a transmitter and receiver typically used to switch between network typed e.g. UTP to fibre transceiver.

Transmission capacity
Similar to bandwidth, a measure of the amount of data a transmission system is able to transmit.

TCP – Transport Control Protocol
Protocol by which applications on networked hosts can create connections to one another, over which they can exchange data in packets. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

UDP – User Datagram Protocol
Protocol by which applications on networked hosts can create connections to one another, over which they can exchange data in packets. UDP provides a faster transmission method but does not provide the reliability of TCP.

UPS – Uninterrupted Power Supply
Sometimes called a battery backup, a device that maintains a continuous supply of power to connected equipment from a separate source when the prime power source is not available.

UTP – Unshielded Twisted Pair
Standard copper-based cabling used for local LAN cable runs, predominantly for Ethernet.

Video encoder
Device for converting analogue video to a digital video stream for network transmission.

Viewing station
A workstation on the network (typically a PC) from which information from network security systems scan be seen such as video, alarm notifications or access control events.

VPN – Virtual Private Network
A private communications network often used by companies or organisations, to communicate confidentially over a public network.

WAN – Wide Area Network
A computer network that allows the connection of LANs and other networks to allow users and computers to communicate from one location to another.

WLAN – Wireless LAN
The implementation of LANs using wire free communication devices. The most common form is based on 'Wi-Fi' as defined by the IEE802.11 standard.