

NETWORKING



COMMUNICATIONS



2020VISION
TECHNOLOGY

ANALOGUE & DIGITAL CCTV

ACCESS CONTROL

SYSTEMS INTEGRATION

**evaluating and choosing
security systems
and the right provider for you**



evaluating and choosing security systems and the right provider for you

Peter Houlis

Managing Director, 2020 Vision Systems Limited

Board Member of the 'Security Systems and Alarms Inspection Board SSAIB and their
Representative on the British Standards Institute (BSI) Technical Committee
Member of the Institute of Directors

Copyright © Peter Houlis 2008



2020VISION
TECHNOLOGY

Contents

Evaluating:

1. Introduction
2. Preamble
3. Security Inspection Bodies
4. Disciplines
5. Intruder Alarms
6. Access Control Systems
7. CCTV
8. Integrated Systems
9. Summary

Choosing your Security Systems Provider:

1. Financial / Economic Standing
2. Technical Capacity
3. Project Experience
4. Aftercare Support
5. Security Consultants
6. Summary

Security System Design:

1. Introduction
2. Intruder Alarm System
3. CCTV System Design
4. Planning & Surveying for CCTV Systems
Survey (General)
System Survey & Design
5. Equipment Selection & Installation
6. Environmental Conditions
7. Brackets & Towers
8. Lenses
9. Cameras
10. Camera Positioning Equipment
11. Cabling
Conduit
PVC or Metal Trunking
Cable Ties
Catenary
Coaxial Cables
Running Cables Together

Access Control Design

1. Design & Specification of Access Control
2. Design & Specification of Systems



2020VISION
TECHNOLOGY

Evaluating

1. Introduction

At a time of rising crime, increases in the severity of criminal attacks and anti social behaviour, teenage gangs and the real and present danger posed by international terrorists and home grown activists, together with the prevalent claims culture and pressure of accountability, the demand for effective security solutions is greater now than at any point in history.

Whatever your walk of life, security in Britain today is of paramount importance. No one can deny the importance of good physical security but the days when it alone could be relied upon have disappeared into the past.

Fortunately, today's security professionals can draw from a substantial arsenal of security options with technology providing many cost-efficient ways to improve security for everyone.

Low cost options can be as simple as locks and barriers, good lighting, staff awareness training and even landscaping.

Technology provides a plethora of electronic security devices such as CCTV, Access Control, Intruder Detection and integrated systems.

World events have created a need for more reliable sophisticated security systems and a demand for more knowledgeable security providers.

This impartial document is intended to introduce you to some of the technology utilised in the war against crime and to help you evaluate and choose your security systems partner, reducing the expensive risk of picking the wrong provider.



2020VISION
TECHNOLOGY

2. Preamble

The UK electronic security industry is largely un-regulated. Anyone can set up a security installation business. There are some first class companies. There are, however, many companies that bring the industry into disrepute. There are thought to be around 4,000 companies, excluding a number of electrical contractors, involved in installing security systems. Along with a few household names whose alarm boxes adorn every high street, the vast majority are SMEs (small-medium enterprises) installing domestic and commercial intruder alarms. Most of them have the ability to install basic CCTV and small Access Control systems but lack the experience to implement and maintain larger more complex systems.

Sadly the intruder alarm no longer addresses all of the security risks prevalent in today's Britain. To secure today's risk requires a more integrated approach and greater use of modern technology.

This has led to a new small breed of security integrators who have the skill levels and knowledge to install and integrate complex 'high end' CCTV and Access Control systems. This does not demean the professional intruder alarm companies or their engineering capabilities, it simply means that the technology involved requires different skill sets, training and a high level of IT and computer literacy.

Unlike the manned guarding industry which is Government regulated by the Security Industry Authority (SIA), the electronic security sector is self-regulated. Of the 4,000 plus companies, approximately 1,800 companies undergo voluntary inspection by one of the industry inspectorates.

3. Security Inspection Bodies

There are two primary industry inspectorates, the National Security Inspectorate (NSI), formally NACOSS, and the Security Systems and Alarms Inspection Board (SSAIB). Both organisations provide Approval and Certification Schemes that are independently assessed, accredited and monitored by UKAS.

Approval Schemes are those which have generally not required UKAS accreditation but which still require providers to demonstrate compliance with relevant British or European Standards, or SSAIB/NSI codes of practice.

Both organisations have minimum criteria for companies wishing to be included on their roll of approved installers.

The SSAIB carry out the following checks, so you don't have to.

- Financial Stability
- Personnel have been screened to the relevant British Standard
- Competence and experience of management and staff
- Insurance cover is relevant to the level and nature of work undertaken
- Premises are adequate for their activity and the security of documentation and records is ensured
- That best-practice standards are maintained and that staff are competent to install the relevant electronic security systems
- That sufficient staff and resources are employed to provide the services offered
- Compliance with the relevant British or European Standards and codes of practice
- That identity cards are carried

SSAIB's skilled assessors regularly check all of the above and the quality of workmanship undertaken to ensure that standards are maintained.

The NSI undertake similar checks and assessments.

You should note that many insurance companies require security systems to be installed and maintained by a company approved by one of these inspectorates.

The industry's premier trade association is the BSIA (The British Security Industry Association). Any company involved in any sector of the security industry can join this organization providing they meet their membership criteria.

The Electrical Contractors Association also has a security systems section under the name Fire and Security Association.

For further information visit:

- www.ssaib.co.uk
- www.nsi.co.uk
- www.bsia.co.uk
- www.fireandsecurityassociation.co.uk



2020VISION
TECHNOLOGY

4. Disciplines

The security field is large and diverse, covering many sectors and disciplines. There are four generally associated with electronic security systems, the most mature of which is the Intruder Alarm, which is well established and governed by well-recognised British and European Standards and Industry Codes of Practice.

5. Intruder Alarms

Traditionally, 'locked up' buildings have been protected by burglar alarms. These generally consist of door and window sensors and movement detectors sited to detect unauthorised entry to a building. Activation of an intrusion device will initiate a signal to a remote monitoring station and/or set off a local warning device.

Protection of external environments such as compounds is a more complex issue involving the use of active and passive movement detectors such as active infra-red beams and microwave fence to cover site perimeters and passive infrared detectors to provide external areas of trap protection. Fence based sensors, including electric fencing and buried wire intrusion devices can be used to provide a higher level of security. Detector activated lighting can also be used to provide an added deterrence.

As stated earlier the intruder alarm industry is well subscribed with a number of both SSAIB and NSI companies providing a high level of service in the provision of intruder alarm systems. A security company that installs commercial and domestic intruder alarms may not possess the necessary expertise in external detection systems, due to the uncontrollable nature of the environment.

However, today many premises require 24 hour access coupled with round the clock protection which has led to the development of access control systems.



6. Access Control System

Restricting access to certain buildings and premises has always been important.

At a time of increased terrorist and criminal threat, insecurity and mutual suspicion, the need to impose restrictions on the access of visitors and staff is paramount in many organisations.

A plethora of valuable equipment, the possibilities of pilfering, the ease of copying and stealing confidential information and personal safety, make Access Control a powerful asset in today's environment.

Access Control Systems are the most efficient method of monitoring activities and limiting/permitting movement across your facility and premises and even to access IT equipment and valuable data. They can be as simple or complex as required and can provide a wealth of management information for security, Health and Safety and Human Resources and give you accountability.

Put simply Access Control is about:

- Who is allowed to be somewhere?
- When are they allowed to be there?
- Where are they allowed to be?

Generally Access Control is used to secure doors to key areas; server rooms, plant rooms, stores, labs etcetera, but can also be used to control entry /egress through barriers, turnstiles and even access to IT equipment like PCs and photocopiers. Modern Access Systems use a variety of technologies, including the latest generation biometric technology: retina scan, finger print and facial recognition through to proximity and hands-free cards and fobs or the latest Smart Cards, which extends the use of Access Control into cashless vending and car park charging. Systems are usually supplemented with Audio and Audio Visual communications and help-point systems.

A well-designed Access Control System provides:

- Improved security for the individual
- Better protection of property and possessions
- Accurate management information about movement in, out or around a facility
- More management control for an organisation
- Effective balance between freedom of access, coupled with the safety of staff and visitors.

When integrated with other security technologies, Access Control becomes a truly powerful site management tool.

7. CCTV

CCTV is a visual surveillance technology designed for monitoring a variety of environments and activities. In the past decade, the use of CCTV has grown to unprecedented levels. Developments in technology have greatly increased its popularity over recent years. As technology has evolved, CCTV is now used not only for security, but also as a management tool assisting Health and Safety, productivity and personnel management.

Digitally recorded images are now of far greater quality. Specific footage can be recalled at the touch of a button, and systems can be integrated with local and wide area networks, allowing images to be viewed from one or more personal computers.

CCTV is also a powerful and effective crime management tool.

Apart from the enormous deterrent value, CCTV has two prime objectives: -

- Proactive – monitored systems allow the spotting of potential problems and a speedy response at the correct level before they become incidents.
- Reactive – the system provides post-incident investigative material. In a car-park scenario, for example, where a car is broken into and two figures are recorded breaking the side window, it is vital for the CCTV to be able to provide identifiable images.

In order to provide an effective CCTV surveillance system solution in large or high-risk environments, it is invariably necessary to utilise both proactive and reactive CCTV.

Generally, the proactive system will contain a number of pan, tilt and zoom (PTZ) cameras strategically located throughout a site and monitored and controlled by security staff from a 24 hour manned control room. With modern transmission medium this can be remote from the site.

The PTZ cameras would generally cover the site perimeter, car parks, roadways, thoroughfares and internal main corridors through areas and high-risk rooms.

To supplement the proactive system fixed cameras would be sited to monitor key target areas and building entrances and exits, in order to provide a visual record of persons entering or leaving an area or building.

As stated earlier, CCTV is a management tool and careful consideration is required to ensure the system meets your objectives.

7. CCTV (cont.)

Before a suitable CCTV System can be specified, it is essential that an initial assessment is undertaken in order to determine the system scope, objectives and requirements. These should not be confused with the technical requirements. It is vital, initially, to provide answers to the following-

- Is the system designed to deter, prevent, detect or prosecute?
- Is it proactive, reactive or both?
- Is it continually manned or unmanned and used only after an incident is reported to provide post incident information?
- What is the scope i.e. prevention and detection of crime, public safety etc. It should be noted that this is a requirement under the Data Protection Act.
- What are the areas to be covered and what degree of coverage is required?

Guidance on producing an operational requirement is given in Home Office publication number 55/06 CCTV Operational Requirement manual – is your CCTV fit for purpose.

BS EN 50132 – 7 1996 titled alarm systems – CCTV Surveillance Systems for use in security applications – part 7 application guidelines, describes fully the steps to produce an ‘operational requirement’ document. This document should clearly state what the customer expects the functions of the system to do. It is designed to encourage clear thinking about what, where, when and by whom and in particular the why of a CCTV System.

The ‘operational requirement’ presents those with the necessary skills to convert the document into a technical specification and test procedures.

Further useful information on CCTV can be obtained from:

The CCTV User Group	www.cctvusergroup.com
The Home Office Website	www.homeoffice.gov.uk
The Information Commissioners Website	www.dataprotection.gov.uk
The Association of Chief Police Officers (ACPO)	www.acpo.police.uk
The Police Scientific Development Branch (PSDB)	www.homeoffice.gov.uk/pcrg/psdb.htm

8. Integrated Systems

The systems integration market is where high-end suppliers excel, with their ability to understand the needs of the customer and translate these into a flexible, well-designed and integrated solution.

Each of the security disciplines mentioned can be integrated to provide operation between systems based on 'cause and effect' or 'what if', then this can provide both a high degree of security and automation in the system making the security officer's job easier.

The benefit of true integration is the seamless operation of multiple technologies working in total synergy to improve efficiency, expenditure and response times.

Examples of the technologies that can be used to create integrated management systems include:

- CCTV
- Access control
- Building management systems
- Perimeter detection
- Traffic barriers
- Pedestrian turnstiles
- Fire alarms
- Intruder alarms
- Asset tagging
- Concierge
- Linking multi-sites

Perhaps one of the most exciting developments in integrated systems is Artificial Intelligence or Video Analytics.

Artificial intelligence adds another dimension to existing and new CCTV systems. Artificial Intelligence, like integration, is designed to remove some of the onus placed upon the CCTV system operators. Using AI, it is now possible to recognize:

- Vehicle registration plates - ANPR
- Faces
- Stationary objects either placed or removed from a scene, even if that scene is busy.
- Direction of movement of people, vehicles or objects.
- People counting and crowd control
- Graffiti
- Behavioural patterns such as slip and fall, loitering etcetera.

Artificial Intelligence can greatly enhance the use, reliability and benefits of both analogue and digital CCTV systems, complementing the overall effectiveness of CCTV by maximizing efficiency of the CCTV operator, making systems more proactive.

9. Summary

Clearly the success of any security strategy starts with a security management plan. The plan should list each department and area, the risk and perceived and actual threats, along with an operational requirement.

Remember to obtain information from the Police Crime Prevention and Anti Terrorist Officer and your insurance company.

Choosing your Security Systems Provider: Points to Consider

1. Financial / Economic Standing

Check financial stability.

1.1 What is the company's turnover in the relevant disciplines and is it relevant to your system requirements? A company installing £1,000 intruder alarms or small CCTV systems may not have the resources or in-house capability to implement larger or more complex CCTV, Access Control or integrated system projects.

1.2 Do they have insurance cover relevant to the level and nature of work undertaken?

2. Technical Capacity

2.1 Do they appear on the SSAIB or NSI list of approved installers, or carry similar relevant third party approval?

2.2 Ask about staff skills, experience, and numbers. Do they have sufficient resources? Are they qualified in the relevant disciplines?

2.2.1 Are staff directly employed?

2.2.2 Are staff vetted and possess ID cards? Do they have corporate clothing so they are easily recognized on site?

2.3 Does the company have the requisite project management skills and adequate resources to implement your project efficiently with the minimum of disruption?

2.3.1 Do they have the in-house technical ability to be able to support the system they are installing? Do they have dedicated installation and service engineers? In many smaller organisations the installation and service engineer is one and the same person, which is not ideal. If he is doing a service call for someone he is not carrying out your installation and vice versa.

2.4 What accreditations, awards and memberships do they hold?

2.4.1 Are they ISO9000:2000 Quality Assured?

2.4.2 Are they registered with CHAS, Construction line, SafeContractor, Linkup etcetera?

2.5 Do they have a procedure for appointing and managing sub-contractors?

2.6 Do they provide, in advance, all makes and models of equipment being proposed? Are all products non-proprietary so you don't get locked into them?



2020VISION
TECHNOLOGY

3. Project Experience

3.1 Can they demonstrate experience in projects similar to that which you require?

3.2 Can they provide at least three customer references for the required discipline in your area / industry sector? Is it a similar size and type?

3.2.1 As well as taking up references, we suggest you make a site visit and take the opportunity to check the general quality of the installation. Looking behind equipment and in control panels is a good indicator of the standard of workmanship. Is the wiring neat, professionally terminated using the appropriate connectors and are cables clearly marked? Nine times out of ten you will find a bird's nest of cables.

3.2.2 Ask the customer if the project was completed on time, within budget and safely.

3.3 Do they have the relevant Health and Safety Documentation, Method Statements and Risk Assessments? Do not be afraid to ask for samples.

3.4 Do they provide you with hand over documentation and a comprehensive O&M Manual? Again, ask for a sample.

4. Aftercare support

4.1 Do they provide a 24 hour, 365 days a year technical assistance line that is manned by trained personnel?

4.2 Do they have a service team with call out engineers available 24/7 365, who are experienced in carrying out repairs on the type of system you have installed? There is little point in sending a burglar alarm engineer to a fault on a major CCTV scheme just to meet call response times.

4.3 Do they hold spares for the equipment they propose to install and do they have a good active relationship with the equipment manufacturer or supplier or do they install 'flavour of the month'?

4.4 Do they provide a comprehensive preventative maintenance support facility with a choice of service levels?



2020VISION
TECHNOLOGY

5. Security Consultants

If you have a large or complex security requirement and lack the necessary in house design skills to draft an operation requirement or security strategy, you might want to consider employing the services of a security consultant. Remember, as with the rest of the industry there is little regulation governing security consultants. Most M&E consultants will offer security consultancy but few have the relevant industry knowledge. Again it is vital to do your home work and choose a consultant with knowledge, experience and a proven track record in the discipline(s) you require.

A good consultant will carry out your risk assessment, assess your budget, prepare the operational requirement and select suitably qualified prospective suppliers to quote for the design and implementation of a system to meet the brief. They can also prepare a full blown technical specification with relevant plans and drawings and carry out a full tender process for the procuring of a suitable system. However, remember the cost of the consultancy service will probably come out of your security budget.

Information on security consultants can be obtained from:

- www.securityconsultants.org.uk
- www.cctvusergroup.com

6. Summary

Choosing a security partner to protect your people and property is a complex business. After all, get it wrong and you have a lot to loose. Always pick a specialist in the discipline you require and do your homework. Quiz the potential supplier about their in-house technical ability and take up references. Remember they will provide you with references from their best customers so make a site visit and visually check the workmanship for yourself. It is well worth the time you will spend.



2020VISION
TECHNOLOGY

Security System Design

1. Introduction

Security is a diverse and complex issue. Remember that security systems and devices are primarily tools designed to do a job of securing your people, property and assets. An Intruder Alarm is simply a device designed to warn of illegal entry. CCTV and Access Control systems are tools designed to provide you with a host of management information. It is therefore important that you focus on what the tool is to be used for. Don't get carried away with the hype, bells and whistles. Make sure your chosen security partner provides the tool(s) that are right for you. The more information you provide the system designer, the more the system can be tailored to meet your brief and deliver the information you require, be it security, Health and Safety or process control monitoring.

Essentially there are two ways of obtaining a CCTV or Access Control System. Both produce an Operational Requirement detailing what you want/expect the system to achieve, leaving the technical design to the potential supplier or consultant. They can produce a full detailed technical specification. If you rely on an Operational Requirement, you have no input into what equipment will be provided and there is every chance that you will get a wide range of quotes to evaluate, which might meet with the brief but fail to meet expectations. You therefore need a reasonable level of technical knowledge to quantify like-for-like options.

Issuing a full and detailed technical specification will ensure that you obtain like-for-like quotes based upon the products and design that best suits your objectives. This however, requires a high level of system design knowledge, as many providers will exploit grey areas within the technical specification for commercial gain and will not accept any design responsibility should the system fail to work or meet expectations.

Below are some things to consider when designing CCTV and Access Control Systems.

2. Intruder Alarm Systems

As stated earlier, Intruder Alarm Systems are the most mature of the electronic security systems and it is well served by a number of reputable providers. Recognised British and European Standards and industry codes of practice govern alarm systems providers. These provide comprehensive guidance for system design. It is also the discipline that requires least input from the user.



2020VISION
TECHNOLOGY

3. CCTV System Design

CCTV consists of a vast and varied array of products and equipment, often sourced from a diverse selection of manufacturers and suppliers, requiring very skilful amalgamation to produce a quality result. Add the firmware and software that are needed for system integration to this mix and it is often beyond the reach of many companies.

Although there is an abundance of non-branded products that often have a high specification and competitive price, it is prudent to stick to well known branded products (JVC, Honeywell, Sony, Samsung, Dedicated Micro, etcetera). This minimizes any issues you may encounter with product support when a system fails.

Remember, anyone designing and implementing a CCTV system needs to take into account the Data Protection Act, The Home Office Guidelines and the National CCTV Strategy.

CCTV is a visual medium and therefore very subjective. Fundamental to any successful CCTV scheme is the need to establish the client's requirements before a system design can be undertaken. The purpose of a CCTV system should be to solve the client's problem. Like the client, you need to consider the system's main objectives. This is achieved through the Operational Requirement detailed earlier. It is from this non-technical brief that the system design will evolve.

Once the purpose and overall objectives of the system have been established, a site survey should be undertaken. It is good practice to obtain a site plan, preferably to scale, or a sketch, which can be annotated with system design considerations. The use of photographs showing camera locations and views is a good idea. This is the time to prepare the outline design specification, detailing camera locations, views and the function of each system component.

There are many important points to consider during the client meetings and site surveys and large or complex projects might require multiple site visits.

The following design check-list, issued courtesy of the SSAIB, identifies some of the design points to be considered.

4. Planning and Surveying for CCTV systems

4.1 Survey (General)

A logical and well thought through approach to planning in both the surveying and the design is essential. Appropriate systems design will have a significant bearing on the performance and reliability of the final CCTV system. It is now a requirement of the Construction (Design and Management) Regulations that the designer shall carry out the design of an installation to eliminate or reduce risks. This includes the risks that may occur during installation, use and maintenance.

4.2 System Survey and Design

4.2.1 There should be a written specification of the system to be installed, incorporating the criteria defined on the operation requirement which should be agreed between the company and the customer and any appropriate third parties such as insurers or other specifiers. The document must be signed by all of the interested parties. At all times the confidentiality of the information should be recognized and maintained. If the specification is designed by or to the requirements of the client or a third party, then this should be clearly recorded in the documentation.

4.2.2 If the specification is to be used by the customer for insurance purposes, it is strongly recommended that the customer obtains agreement in writing from the insurance company that they are happy with the specification/operation requirement, before work commences on the installation.

4.2.2.1 Any changes to the specification or the method of operation of the system after agreement of the contract should be agreed in writing by all interested parties and re-confirmed on the service visits.

4.2 System Survey and Design (cont.)

4.2.3 The specification for a particular CCTV installation will depend on several issues, including:

4.2.3.1 The risks

4.2.3.2 Type of surveillance required e.g. daytime only or 24/7

4.2.3.3 The level of detail to be displayed and/or recorded e.g. is facial recognition required.

4.2.3.4 Transmission systems and media

4.2.3.5 Level of surveillance

4.2.3.6 Is vandalism likely to be a problem e.g. equipment damage?

4.2.3.7 Type and usage of the area/building to be observed

4.2.3.8 Lighting issues e.g. sunlight/low light/no light

4.2.3.9 Responsibility for installation of any additional lighting required

4.2.3.10 Maintenance of the system

4.2.3.11 Safety of maintenance staff

4.2.3.12 The required response

4.2.4 Bearing this in mind, several parties may need to be consulted at the initial survey / design stage including:

4.2.4.1 The client or end user

4.2.4.2 Insurers (if applicable)

4.2.4.3 Police (if applicable)

4.2.4.4 Specialist security consultants (if applicable)



2020VISION
TECHNOLOGY

4.2 System Survey and Design (cont.)

4.2.5 To establish this process, the client or end user's objectives and expectations are fundamental in designing a system that is fit for their purpose. These expectations will constitute the basis of the system's operational requirement. It is recommended that all interested parties meet on site at the earliest stage of planning and design so that the requirements for surveillance can be established. If this is not possible, it is strongly advised that the appropriate interested parties visit the site and make known their views and recommendations prior to the commencement of the installation. It is also recommended that all interested parties should retain copies of documentation and correspondence relevant to the project.

4.2.6 The following points should be considered when surveying and designing a system:

4.2.6.1 The camera and lens combination proposed should give adequate performance under all intended lighting conditions.

4.2.6.2 The environmental conditions in which a camera is to operate should be taken into account.

4.2.6.3 The selected camera position allows for security and maintenance.

4.2.6.4 Vulnerable to vandalism or other attack.

4.2.6.5 Consideration should be given to camera position and performance at certain times of the day or night (e.g. low sun at dawn and dusk, bright lights at night, seasonal variations etc. that may require extended sunshields).

4.2.6.6 The camera mounting brackets, towers, poles and their fixings should be adequate to support the weight of the camera and any co-mounted hardware. The effect of the wind pressure on the completed assembly should be considered for safety and image stability reasons.

4.2.6.7 The lens chosen covers the area to be viewed and provides the correct level of detail specified e.g. the identification/recognition of a Rotakin or equivalent.

4.2 System Survey and Design (cont.)

4.2.6.8 The lens format is compatible with the selected camera.

4.2.6.9 The intended size and number of monitors/displays takes into account operator viewing distance and fatigue (“monitor blindness”).

4.2.6.10 Ensure compensation has been made for any unacceptable signal loss that may result from the transmission distance between cameras and monitors.

4.2.6.11 The control equipment, recorder and monitors etc are suitably positioned to take account of the environmental conditions and ease of use

4.2.6.12 The control equipment takes into account any foreseeable future requirements.

4.2.6.13 The system can be easily controlled and monitored by the operator(s).

5. Equipment Selection and Installation

Below we consider the details of hardware selection and its installation.

6. Environmental Conditions

Equipment should be selected and/or installed to withstand the following air temperatures:

6.1 Internally sited equipment, 0 to 40 degrees C

6.2 Externally sited equipment, -20 to 50 degrees C

Note: equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding, or extra cooling, may be required in such circumstances. Exterior graded equipment should be considered for use in unheated premises.

Where equipment is exposed, it should meet a minimum of IP60 or, in a particularly exposed location or tunnels, IP66 as specified in BS EN60529.

For all items of equipment to be used, the following should be taken into consideration.

6.2.1 Temperature

6.2.2 Humidity

6.2.3 Dust and other air contamination

6.2.4 Vibration

6.2.5 Electrical interference

6.2.6 Rigidity, taking into account high wind velocity

6.2.7 Ease of safe access for installation, maintenance and service

6.2.8 Convenience of operator use.

7. Brackets and Towers

Brackets and towers should be specified to take account of the following points:

7.1 The maximum load to be carried by the bracket or tower.

7.2 The possibility of the camera assembly being used as a bird perch must be considered, especially where large birds, such as seagulls, may be present.

7.3 The effects of high wind speeds on the windage area of the equipment to be mounted on the tower or bracket.

7.4 For towers and columns, the ground conditions must be established to enable correct design of the foundation

7.5 The height at which the equipment is to operate.

7.6 Wherever possible “tilt over” or “wind down” towers should be used so enabling all maintenance of equipment to be carried out at ground level.

7.7 Before erecting brackets and/or towers the following points should be taken into consideration and manufacturers’ specifications and recommendations should be followed:

7.8 Planning permission (where applicable the customer is responsible)

7.9 Temperature (with regard to distortion of alignment)

7.9.10 Rigidity (taking into account high wind velocity)

7.9.11 Corrosion resistance having regard to any specific local conditions

7.9.12 Possibility of damage from lightning (BS EN 62305 refers)

8. Lenses

Lenses should be specified to take account of the following points:

The lens mount (C or CS) should match that of the camera. An adaptor should be considered.

The lens angle should be selected to give the required 'field of view' and image size required (identification/recognition etc.).

Unless lighting levels are almost constant, it is recommended that the lens has an adjustable iris control, even when using an Electronic Iris.

It is recommended that lenses used on cameras subject to wide variations of light levels is fitted with an automatic iris to control the light levels reaching the sensor.

Due to extreme ranges of lighting levels, a neutral density (ND) spot filter should be incorporated.

Lenses for day and night use shall be set up using ND filters to set the "back focus" to avoid pictures going out of focus at night. Zoom lenses shall also be set up using ND filters to ensure zoom tackling is achieved. Where lighting levels are lower the use of aspherical lenses should be considered.

9. Cameras

Cameras should be mounted in serviceable positions, free from obstructions and, wherever possible, not directly viewing bright light sources. Wired connections should wherever possible be concealed. Mechanical protection should be considered e.g. metal conduit or flexible conduit on movable cameras where physical damage is a possibility.

Cameras should be specified to take account of the following points: -

9.1 Video output should be 625 lines CCIR standard with colour encoding being PAL, when used in the UK unless otherwise required by the specification.

9.2 The signal to noise ratio should be greater than 43dB, under normal conditions of operation with the AGC control off.

9.3 The minimum sensor illumination should be stated in Lux to achieve a full video input.

9.4 The lens mount (e.g. C or CS) should be compatible with the required lens.

9.5 Auto iris output, either video or direct drive, must be compatible with the chosen lens.

9.6 All cameras must be clearly marked with their operating voltage.

9.7 The environmental conditions in which a camera is to operate should be taken into account when choosing the camera housing.

9.8 The camera and its support hardware should be securely mounted taking into consideration the long-term effects of vibration.

9.9 Where supplementary lighting is to be used, the spectral response of the camera should match that of the lighting.

9.10 Where day and night use of a camera is required, the use of the colour/monochrome switching cameras is recommended.

10. Camera positioning equipment

Mechanisms should be specified to take account of the following points:

- 10.1 The maximum required pan and tilt rotation in degrees or if continuous rotation for pan is required.
- 10.2 The establishing of “no-view” sectors if required to comply with Data Protection (privacy) recommendations issued by the Office of the Information Commissioner
- 10.3 The effective rotational speeds of the intended targets should be known
- 10.4 The required rotational speeds of pan and tilt or if proportional or variable speeds are required.
- 10.5 The maximum load and the rigidity, taking into account high wind velocity.
- 10.6 For aesthetic reasons, domes may be considered. When choosing domes the following points should be assessed: -
 - 10.6.1 The optical correctness of the dome.
 - 10.6.2 The lens moves concentrically within the dome.
 - 10.6.3 The loss of light through smoked or mirrored domes.
 - 10.6.4 Internal reflection.
 - 10.6.5 How will the dome be cleaned if externally mounted?
 - 10.6.6 It is recommended that in the interests of safety, extra low voltage mechanisms are considered.
 - 10.6.7 Where equipment moves under normal operation (e.g. pan/tilt camera), a warning notice should be affixed adjacent to the assembly indicating the dangers of movement without warning
 - 10.6.8 The manufacturer's recommendations should be followed and consideration should be given to the method of mounting and possible requirements for safety restraining chains (or similar).

11. Cabling

11.1 Where any work is required on any mains supply circuits, the requirement of BS7671 (formerly the “Requirements for Electrical Installations” issued by the Institution of Electrical Engineers now the Institute of Engineering and Technology) shall be met.

11.2 All interconnecting cables should be fixed and supported and installed to conform to good working practices.

11.3 Suitable fixings and supports can include:

11.3.1 Conduit: When metal or plastic conduit is used, suitable bushes or grommets should be fixed to each end to prevent damage to the cable. Where metal conduit is cut any protective medium, such as galvanise shall be repaired. When conduit is used to carry the cable it must terminate as close as possible to the unit to be connected.

11.3.2 PVC or metal trunking: Where trunking is used to carry the cable it should terminate as close as possible to the unit to be connected. Where conduit or trunking is used, the manufacturers recommended capacity of the containment must be observed.

11.3.3 Cable ties: Where cable ties are used, they shall not be over tightened because of the possible damage to the performance of coaxial cables.

11.3.4 Catenary: When overhead catenary wires with loop holders or plastic buckles are used the supporting wire should be securely attached to the fabric of the building.

11.3.6 Coaxial cables: The maximum length of cable run should not exceed the distance which equates to a loss of 6dB at 5.5MHz for the entire length or run including switching and monitors etc. All coaxial cable shall be 75ohm characteristic impedance.

11.3.7 Running cables together: Care should be taken to keep signal cables separated from mains cables, because of the risk of induced effects. When CCTV cables are to be run within cable containment systems containing main cables, the IEE Regulations concerning segregation should be observed.

11.4 All cables should be of the type and size appropriate to the application and should take account of transmission rate, electrical interference and voltage drop.

11.5 The supervised premises shall be surveyed using the principles of the OR as advised by the HOSDB.



Access Control Design

1. Design and Specification of Access Control

Access Control is the modern equivalent of the tried and trusted lock and key over which it provides many advantages. Keys can be lost resulting in the costly and inconvenient replacement of locks, especially if a key is suited to a number of locks. Electronic Access uses codes, cards or fobs and even biometrics that can be simply deleted from the system. So if a card is found it will no longer offer access, unlike a key.

Generally Access Control provides an audit trail of who, when and where. Providing you with accurate information on movement in out or around your facility by staff and visitors. Thus providing more control for an organization.

Access Control has two levels of system. Stand-alone and PC based networked system. It is very important to clearly identify what is needed from the system so the correct type of system is specified.

PC based networked systems offer total control to an organization, recording all events and providing reports on all movements/transactions on the system. All administration and programming is carried out from a central point where all cards and fobs et cetera can be granted access through varying doors, with different time profiles on different days. All events are logged and the software provides detailed reports based upon individual users, doors, times and dates etc.

Care is needed when choosing PC based systems to ensure the correct system is specified. Some systems are suitable for 1 or 2 doors, some for tens of doors and others for hundreds of doors.

Stand-alone systems are simple and very easy to install and programme, offering good security on small areas but often lack the reports and management information provided by PC based systems.

The following design check-list issued courtesy of the SSAIB identifies some of the design points to be considered.

2. Design and Specification of Access Systems

2.1 There should be a written specification for the system to be installed which should be agreed between the company, customer and any appropriate third parties such as insurers or other specifiers. At all times the confidentiality of the information should be recognized and maintained. If the specification is designed by, or to the requirements of the client or a third party, then this should be clearly recorded in the documentation.

2.2 If the specification is to be used by the customer for insurance purposes, it is strongly recommended that the customer obtains agreement in writing form the insurance company before work commences. Once again, confidentiality should be maintained.

2.3 Similarly, it is essential that the requirements of any local Police/Fire policy be strictly adhered to and that the local Police/Fire Authority be kept informed in respect of new, altered or removed/discontinued systems and keyholder changes where applicable.

Systems which could impede exit from a premises or area should be designed with the utmost attention paid to the evacuation needs of the premises in the event of fire or other emergency. Such systems should be designed to be “fail-safe” i.e. “fail-open”.

Alternatively systems should be designed such that access-controlled fire doors are released in the event of the activation of the premises fire alarm.

Interconnection of the customer’s fire alarm system should be done in co-operation with the fire alarm’s installation and/or maintenance contractor, and in accordance with BS 5839. In case of doubt, customers should be advised to seek guidance from the local Fire Service.

Specifications and contract documentation should clearly define the precise point at which responsibility for the interconnection divides between the fire alarm’s installation and/or maintenance contractor and the access control supplier.



2. Design and Specification of Access Systems (cont.)

2.4 Any changes to the specification or the method of operation of the system after agreement of the contract should be agreed in writing by all interested parties and re-confirmed on service visits.

2.5 When surveying the premises and writing the specification, the following should be considered:

2.5.1 Is vandalism likely to be a problem e.g. equipment damage?

2.5.2 Utilisation of the premises, i.e. type of business operated.

2.5.3 Adjoining properties. i.e. is there access from the premises?

2.5.4 Does the client have specific requirements? i.e. time controls, disability factors to be taken in to account.

2.5.5 Are any additional security measures required? i.e. CCTV, intruder alarms.

2.5.6 Consider the Disability Discrimination Act i.e. persons with sight impairment, dexterity problems, wheel chair users and the mounting height of equipment etc.

2.5.7 Access through barriers i.e. opening, closing times, barrier types.

2.5.8 Type of tokens available, for example:

2.5.8.1 Digital (PIN Code)

2.5.8.2 Key

2.5.8.3 Card entry

2.5.8.4 Proximity

2.5.8.5 Combined Digital and card entry

2.5.8.6 Biometric

2.5.8.7 Combinations of the above



2. Design and Specification of Access Systems (cont.)

2.5.9 Reader types available:

2.5.9.1 External

2.5.9.2 Internal

2.5.9.3 Swipe

2.5.9.4 Insert

2.5.9.5 Proximity

2.6 Choice of system to be offered in relation to facilities available and/or as required, e.g.

2.6.1 Level of Security

2.6.2 Volume of use combined with speed of operation

2.6.3 Transaction recording (on-line / off-line)

2.6.4 Expandability

2.6.5 Programming ease

2.6.6 Deletion and/or addition of users

2.6.7 Number of users and possibility of future expansion

2.6.8 Anti pass back

2.6.9 Duress code

2.6.10 Door open

2.6.11 Door forced

2.6.12 Door timer

2.6.13 Egress facility

2.6.14 Alarm inputs

2. Design and Specification of Access Systems (cont.)

2.7 Doors, Locks and Releases, for example:

2.7.1 Type and structure of doors and frames

2.7.2 Type of locks

2.7.3 Type of releases

2.7.4 Type of door-closer

2.8 Type of barriers:

2.8.1 Sliding gate

2.8.2 Swing gate

2.8.3 Rising arm barrier

2.8.4 Rising kerb / bollard

2.8.5 Turnstiles

2.8.6 Paddle barrier

2.8.7 Air gates

2.9 The initial specification of a system should take account of the design criteria, ease of use, the quality of the equipment provided, a high standard of appearance of the installation, compatibility of the equipment and possible future extension of the system. In all cases, the power supplies, both main and standby, should have 30% spare capacity when the system is installed.

2.10 When a system is designed for use in a new building, it is essential to involve the building's designers with a view to producing a system that has a minimum disruptive effect on the use of the unfinished building

2.11 The terms of the contract between the company and the customer should make it clear whether the equipment is purchased or leased and should state the period of warranty. A maintenance agreement should follow immediately after a warranty period and should be amended where necessary to allow for increased frequency of visits. The maintenance agreement should cover a period of at least one year.

2. Design and Specification of Access Systems (cont.)

2.12 The specification should define:

2.12.1 Type of access control to be provided (If this is limited by the customer's choice. This fact should be recorded.)

2.12.2 Utilisation of premises when the system is in use, e.g. unoccupied, partially occupied, fully occupied.

2.12.3 Location of equipment, including mounting heights.

2.12.4 Cable routes.

2.12.5 Entry and exit routes.

2.12.6 Criteria and restrictions on the use of the system.

2.12.7 Size and capacity of power supply (see also 3.6 above) and stand-by capability.

2.12.8 Responsibility for providing a 230v AC supply, and a clear demarcation of responsibility.

2.13 The specification should indicate that a full commissioning test will be undertaken on completion of the installation.

2.14 On acceptance of the specification, the customer should sign a form of acceptance or contract to indicate that he/she has read the specification and understands the extent of the facilities to be provided by the system.



Conclusion

I hope you have found this document both interesting and useful in your quest to obtain the correct security system and provider to satisfy your needs.

Should you require more personal advice or any additional information please do not hesitate to contact me, Peter Houlis, or one of our able team at:

2020 Vision Systems Limited

28 Northumberland Square
North Shields
Tyne and Wear
England NE30 1PW

Telephone: **+44 (0)191 296 2662**

Website: **www.2020cctv.com**

e-mail: **phoulis@2020cctv.com** or **sales@2020cctv.com**

a: 2020 Vision Systems Ltd
28 Northumberland Square
North Shields
Tyne & Wear
NE30 1PW

t: +44 (0) 191 296 2662
f: +44 (0) 191 296 2661

e: sales@2020cctv.com
w : www.2020cctv.com