National Security Inspectorate
Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY
E: nsi@nsi.org.uk | W: nsi.org.uk

Date: 29 November 2017

To: All NSI NACOSS Gold and Systems Silver approved companies and applicants

TECHNICAL BULLETIN No: 0041

NSI Code of Practice NCP 104 Issue 3 for the design, installation and maintenance of CCTV surveillance systems

NSI Code of Practice NCP 104 Issue 3 has a publication date of November 2017 and is available from the NSI website or on request.

Withdrawal and implementation timescales for approved and applicant companies

You can install systems to NCP 104 Issue 3 as soon as you are able to comply with the requirements and NCP 104 Issue 2 will be withdrawn from use on 1 May 2019. All contracts entered into after this date will have to comply with the requirements of NCP 104 Issue 3. During the transition period, where deviations are identified during technical site inspections, we will continue to raise all nonconformities as Improvement Observations or Improvement Needs regardless of the NCP 104 Issue followed. However, where appropriate, we may raise Audit Notes against NCP 104 Issue 3 installations, where we identify process related issues.

Note regarding the status of NCP 104 Issue 3

Although based on the structure of BS EN 62676-4:2015, NCP 104 Issue 3 omits a number of the requirements of this standard, such as the grading of systems and certain aspects of image quality testing. Therefore compliance to NCP 104 cannot be used to claim compliance to BS EN 62676-4:2015 or any of the associated BS EN 62676 series of documents.

Details of the content

This Technical Bulletin should be read in conjunction with the Code of Practice.

Where the actual wording of the standard is quoted, it is reproduced in bold text.

Where it is considered relevant to further clarify the specified requirement, additional guidance is included in italics.

We will consider alternative methods of achieving compliance with specified requirements where these can be demonstrated to be equivalent.

Introduction

NCP 104 has been revised and reissued primarily to account for the withdrawal of BS EN 50132-7:1996, which was directly referenced in NCP 104 Issue 2. This revision of NCP 104 is based on the structure and content of BS EN 62676-4:2015, which has replaced BS EN 50132-7 and introduces a design philosophy similar to that proposed in the Home Office Scientific Development Branch (HOSDB) document, 'CCTV Operational Requirements Manual 2009 Publication No 28/09'. Both documents advocate that an Operational Requirement (OR), which captures the user's security needs, is created prior to the design and installation of a system. The system design, test and commissioning is subsequently developed from the OR.

In this issue of NCP 104, we have chosen to use the term CCTV surveillance system (or CCTV system) due to the fact that the term 'CCTV' is widely used. If you prefer, you can use the term 'video surveillance system' (VSS) to describe the solution you are offering provided it does not lead to misunderstandings with customers such as implying or inferring compliance with BS EN 62676.

In this issue of NCP 104, the term Operational Requirement has been replaced by the term User Requirement (UR). The intention is that this will focus the attention of security companies on the user's needs regarding the system to be designed and installed. However, where customers require or security companies prefer, the term Operational Requirement may be used.

The revision of NCP 104 also allowed for a 'technology and terminology update' to bring the language in the code of practice up to date and to introduce requirements for design areas, such as network security, detectors, video analysis, audio and cabling, that are not covered in BS EN 62676-4:2015.

The code of practice contains a number of documented procedures that must be carried out as part of the development process (risk assessment, site survey, user (operational) requirement, system design specification, test plan). The resulting documents can be amalgamated if it is practical and appropriate to do so. For example, on simpler CCTV systems, the risk assessment, site survey and user requirement may be produced as a single document for presentation as part of a costed proposal. Should the proposal be accepted, then the system design specification and test plan can be completed. For more complex systems, or for particular customers or contracts, it may be necessary to present these as individual documents. The decision to select one or more ways and means to present documentation is for the security company.

Where the user provides any of the required documentation, such as architect's drawings, security consultant's risk assessment and design, customer generated user requirements, and so on, these should be included in the security company's documentation where possible. Where this is not possible, a reference should be made to these documents within the system design specification.

1. Scope

There have been no changes to the scope of NCP 104 apart from moving away from BS EN 50132-7. You are however reminded that compliance to NCP 104 on its own does not meet the requirements of BS EN 62676-4 and any of the other BS EN 62676 documents.

2. References

References have been updated to include:

- BS EN 62676-4:2015 Video surveillance systems for use in security applications. Application guidelines.

3. Terms and definitions and abbreviations

NCP 104 includes the following terms and definitions:

3.1 Terms and definitions

3.1.1 CCTV surveillance system

A security system using a combination of hardware and software to provide the images (and audio where required) necessary to perform a safety or security function.

3.1.2 Customer

An individual or organisation entering into a contract with a security company.

3.1.3 Operational period

A time period over which all or part of the CCTV surveillance system is required to function to meet the user requirement.

3.1.4 Security company

An organisation contracted to provide the design, installation and/or maintenance of a CCTV surveillance system.

3.1.5 System owner

An individual or organisation responsible for the control and management of a CCTV surveillance system.

3.1.6 Operator

An individual trained and authorised to operate all or part of the CCTV surveillance system.

3.1.7 User

A customer, system owner or other organisation responsible for defining the scope of the CCTV surveillance system.

3.1.8 User requirement

A document which defines the functions of the CCTV surveillance system.

Note: *May be referred to as the operational requirement*.

4. Risk assessment

NCP 104 contains a new requirement for a risk assessment to be carried out and documented. The risk assessment must address the security needs of the user and any requirements necessary to protect the system from accidental or malicious actions.

During the risk assessment, consideration must also be given to the threat of the CCTV system being reduced in capability or disabled through accidental or malicious actions. You must mitigate or identify to the customer any risks to the continuing operation of the system.

The risk assessment can be a standalone document or it can be included in the user requirement (UR) document or System Design Specification (SDS). NCP 104 Appendix A contains a sample risk assessment form.

Where the user provides the risk assessment, it should be included in your documentation, if possible, or a reference should be made to the risk assessment in the UR/SDS.

5. Site survey

NCP 104 retains the need to carry out and document a site survey. This site survey may be carried out as part of the risk assessment process and the results can be included in the UR/SDS. This clause contains a number of requirements that are to be included in the site survey. Where it is not possible to visit the site any assumptions or approximations that may affect the design of the system must be included in the SDS.

Where it has not been possible or it is not considered either practicable or necessary to carry out a site survey (for example the system design has been provided by the user or where the property has not been built), this fact and any limitations that may affect the design of the system (for example, expected lux levels, proximity of adjacent properties, changes in internal layout), must be made clear in the system design documentation.

Where the user provides the site survey, it should be included in your documentation, if possible, or a reference should be made to the site survey in the UR/SDS.

NCP 104 Appendix B contains a sample site survey form.

6. User requirement

The UR is not the system design. The UR is a list of security needs (WHO, WHAT, WHEN, WHERE, WHY) based on the threats identified in the risk assessment in the area(s) defined in the site survey that the user wants the system to address. Once these needs are understood a system (HOW) can be designed to meet them.

The requirement to develop and document a UR is a significant change in the process of designing a CCTV system. In the previous code of practice, based on BS EN 50132-7:1996, there was no specific requirement to develop a UR/OR in all cases and designs would be based on whatever documentation and system operational criteria might be available.

In BS EN 62676-4:2015, the emphasis is on the designer to obtain from the user, as part of an information gathering process, their requirements in terms of; what do they expect the deployment of the system to achieve, what they will see, when they will see it and what they will do with the information captured.

Clause 6 of NCP 104 contains fifteen sub-clauses and, although some requirements may not be applicable to all scenarios, it is the designer/surveyor's responsibility to ensure all relevant requirements are captured and documented based on discussions with, or on other information provided by, the user.

The contents of a UR are fundamentally answers provided by the user to a list of questions that relate to the functions of a CCTV surveillance system. In some cases, the UR will be provided by the customer or a consultant. If this is the case, you should check your understanding of the requirements to ensure these are valid before committing to a system design.

Where no UR is provided, this needs to be developed in discussion with the customer. Potential ways to achieve this are:

Create a list of the requirements in Clause 6 and check these off during the risk assessment and site survey process. Where a requirement is not covered during these activities, further discussion with the customer may be required.

Provide a list of the requirements in Clause 6 to the customer as a questionnaire prior to any visits so they can develop their own UR. The risk assessment and site survey activities should be able to validate/clarify the requirements.

7. System design

You must document the system design in a fully documented SDS. The SDS must have a unique reference number and a means to identify revisions caused by any design changes.

A fully documented SDS should include a description of all system components (cameras, detectors, illumination, network, record, store, display, power supplies, support structures and cabling), details of the system configuration (image categories, fields of view, frame per second, video resolution, video, audio and export formats, triggers and alerts (cause and effect), storage capacity, encryption, data compression, metadata, network topology, network capacity, technical and physical network security, tampers, back-up power supply capacity and details of any hardware, interface protocols, cabling and so on required to integrate into connected systems and networks), training to be provided and preventive maintenance schedule.

During the system design process, you must discuss with the user any limitations identified which prevent the UR from being met in order to agree any resolutions. Any changes to the UR and any subsequent changes to the system design must be documented.

The agreed system design must be fully documented in a SDS which must be signed off by the customer or the customer's representative.

Design is the process of taking the UR and translating this in to a system specification that will fulfil the user's security needs.

Where existing infrastructure (networks, power supplies, equipment racks, support structures, containment, and so on) is to be used to meet the system design, this should be stated in the SDS.

Where specific requirements are placed on the customer, such as the provision of electrical services or civils or assumptions/expectations about services provided by the customer are made, then these should be included in either the SDS or contract.

During the system design phase, consideration should be given to the capability of the individuals who will be using the system. Allowances in system design should be made for individuals who may be physically impaired or who may have difficulty interacting with PC based systems.

7.1 Legislation and standards

The SDS must draw the customer's attention to the Data Protection Act and the information available from the Information Commissioner's Office.

The General Data Protection Regulations (GDPR) will come into effect on the 25 May 2018, when the Data Protection Act (DPA) 1998 is due to be repealed in favour of new UK legislation.

The majority of CCTV systems, commercial and residential, will be subject to the DPA/GDPR and, whilst it is not your responsibility for ensuring the system owner complies with the DPA/GDPR, you should ensure the system can comply with the DPA/GDPR and advise your customer to look at CCTV guidance on the Information Commissioner's website (www.ico.org.uk) to review their responsibilities under the DPA/GDPR.

Legislative requirements within both the Town and Country Planning Act and Clean Neighbourhoods and Environment Acts have a bearing on what is and is not permitted in system design. You should make yourself aware of the limitations imposed by this legislation as these may, if contravened, result in a requirement to redesign or reconfigure the installed system.

7.2 Site plan

A site plan must be included in the SDS which details the locations of interest (risk areas and targets) and key system components, including: cameras (including field of view and distance to risk areas and targets), detectors (including range and coverage), illumination (existing and additional) and control equipment (monitor and record).

The site plan may be a line diagram or a marked up photographic/video representation of the proposed location detailing the required information as either graphics or as a written description.

For simpler systems this need only be a line drawing with target areas, proposed placement and coverage of cameras and detectors, maximum distances of cameras and detectors from target areas, location of existing or proposed illumination and the proposed location of all other system components. For complex systems, more detail may be required. The site plan may also be a more detailed mark-up of the site survey document carried out in Clause 5 of NCP 104 or a marked up copy of building documents. It is important that the customer understands the coverage of the system and where the system components will be located.

7.3 Camera equipment and 7.4 Functional cameras and 7.5 Equipment housings and 7.6 Field of view/object size

Lens and camera combinations must be selected to ensure resolution, object size, field of view and illumination performance meets the UR.

In some circumstances, the UR may contain a requirement that may not be possible to achieve using one or even a number of cameras in one location and it may be necessary to site cameras in different locations to achieve the objective. For example, if the requirement is to identify shoplifters in a large retail complex, it may be difficult and very expensive to provide this level of surveillance in all areas. The same may be achieved by ensuring targets can be identified

as they enter or exit the surveillance area and provide sufficient coverage inside the area to observe their movements and actions and correlate the images.

Table 1 in Appendix C provides general guidance on the likely percentage size of the target as a measure of display size. However, Table 1 should be used carefully because some targets meeting the percentage size may not meet the image category requirements due to poorly configured equipment or adverse environmental conditions. Equally, in ideal conditions, a target that is smaller than the guidance percentage figures may meet the UR.

Lens and camera combinations must be selected to ensure resolution, object size, field of view and illumination performance meets the UR.

Details of the field of view and maximum distance to the target can be noted on the site plans.

Details of any specific image categories and coverage at pre-set positions should be included in the SDS.

These details may be included in the site plan.

Where additional camera housings are used, you should retain details of the equipment and any claims of conformity for IP ratings, and so on.

Where technical information is included in manufacturer's data sheets, these can be cross-referenced to an annex in the SDS or other readily available resource containing this information. Be cautious when using manufacturer's websites as information resources because documents may be moved or removed when a product becomes obsolete.

7.7 Detectors, video analysis, triggers, alerts and thermal imaging

Detection areas must be within the associated cameras field of view.

Detectors must be able to cover the area where targets are required to be detected.

Detectors must be positioned so that activity outside of the target area does not cause activations.

Consideration should be given to equipment placement, coverage and configuration when using detectors, video analysis and thermal imaging to generate triggers and alerts. Poorly configured detection may cause an overload on operators or, by generating excessive alerts, video and/or data, make the system unusable. Similarly, a lack of effective detection may cause the system to fail to meet the UR.

Triggers and alerts generated by detectors and video analysis must meet the requirements and/or responses identified in the UR.

Any cause and effect stated in the UR should be clearly documented in the SDS. This may be detailed against the equipment specification (for example, the associated camera or detector) or as separate list.

7.8 Illumination

Existing illumination must be assessed for levels, direction, spectral content and hours of operation.

Failure to provide sufficient illumination, with the correct spectral content and contrast, across the area under surveillance, will almost certainly prevent some aspects of the UR being met. Therefore, significant effort should be taken to ensure that any shortfalls in the quality or availability of illumination are identified early in the requirements capture process so that a suitable solution can be provided.

Requirements for additional illumination must be determined.

Types and locations of illumination should be stated in the SDS or a global statement made if ambient lighting is to be used across the site. This information can be included in the site plan.

Where there may be insufficient lighting to meet the UR, this should be identified to the customer to either resolve or be accepted as a limitation and noted in the SDS.

Where there is a requirement to capture moving targets in detail, camera shutter speeds may have to be increased and this may subsequently require an increase in the level of illumination necessary to meet the UR.

7.9 Video/audio performance and 7.10 Video frame rate and 7.11 Video resolution

Configuration settings that have an impact on the quality of images must be set to ensure the UR is met.

The format in which images are transmitted, stored and exported from the system must be selected after discussion with any stakeholders.

Video configuration settings (format, frame rate, resolution) for cameras and video recorders should be documented in the SDS.

Where configurations settings are global, i.e. each camera in the system has exactly the same setting, this can be included as a global configuration setting in the SDS. Exceptions can be identified for specific cameras.

7.12 Storage and 7.13 Data compression and 7.14 Encryption and 7.15 Metadata and 7.16 Image enhancement

The total system storage requirements must be estimated before a system is installed so that appropriate memory capacity can be specified.

System storage requirements will be based on the quality and quantity of data captured and the retention period set.

The SDS should include either calculations or assumptions to support decisions made on the storage required to meet the UR.

Additional compression of the data should not affect the quality of the images or metadata.

Where storage capacity may be an issue, provision of a means to prune unwanted data, as opposed to the compression of all data, should be recommended to the user.

Consideration must be given to the need to encrypt data at rest and data in transit.

Data should be encrypted using publically available encryptions methods and should not alter the quality of the data during the encryption/decryption process.

Metadata requirements identified in the UR should be included in the SDS.

Image enhancement tools must not change the original recording.

Where an enhanced image is exported, an audit trail documenting changes to the original image must exist.

This audit record may be provided as part of the application software.

7.17 Image export

Data exported from a recorder must have no loss of individual frame quality, change of frame rate or audio quality.

The system must not apply any format conversion or further compression to the exported images.

Preferences for the export format and media type used should have been identified in the UR. Where these have not been identified, or the customer is unsure, you should make your best judgement when specifying the system, taking into account the likely size of data files and any local police force requirements.

Unless a preference has been stated, exported data should be able to be played on widely available software, such as VLC.

7.18 Displays

Monitors and other viewing devices must be selected and positioned to meet the requirements of the operator's task(s).

Consideration should be given to ensuring the aspect ratio (4:3, 16:9, and so on) of the video format can be viewed without distorting or cropping images.

7.19 Network and transmission equipment and 7.20 Network security

The system designer must select the most suitable internal (LAN) and external (WAN) communications infrastructure.

Where you are responsible for the provision of the network, the network must be designed to ensure data is not lost or corrupted during transmission and that images presented for viewing and storage are not subject to any jitter or delay that may affect the UR.

Network requirements must be stated in the SDS for all external connectivity and shared networks.

Network requirements for shared networks include the likely data transfer/bandwidth loading on the host systems and the data protocols and interfaces to be used. Therefore, where you are sharing or connecting to an external network, you must calculate/assess the likely internal and external traffic bandwidth requirements of the system and either state what data protocols and interfaces you require the customer to provide or state how you intend to interface into the customer's network.

The SDS should document details of the physical system topology including port numbers. This may be included as part of the site plan.

After the provision of images, effective network security is possibly the next highest priority to be considered in the system design process. All physical and logical network endpoints and processes running on the system may offer an opportunity to access and exploit or interfere with data on the system or be used as a vector to attack attached systems.

You should document all means taken to mitigate these risks and/or provide recommendations to the customer to ensure the security of the network is maintained.

7.21 Tamper and 7.22 Backup power supplies

Cameras must be installed in such a manner to reduce the opportunity to change the field of view of the camera and access cabling.

The ability to be able to deter, detect and/or prevent external acts, either malicious or otherwise, affecting the continuing effectiveness of the system should be based on the resilience requirements identified in the UR and appropriate mitigations put in place.

Uninterruptible power supplies (UPS) must be provided to those system components necessary to support specific functions identified in the UR.

The means to mitigate all tamper and power supply risks identified should be documented in the SDS.

Where requirements are met using specific equipment, for example cameras with anti-tamper fittings or tamper detection, this may be included in the equipment details. Where specific requirements need other means to provide resilience, such as anti-climb measures or suitable containment, these can be documented within a separate section or annex in the SDS.

7.23 System integration

Integration must not have a detrimental effect on connected systems or host networks.

Where systems are integrated, consideration should be given to ensuring network connections and associated data traffic does not adversely affect any connected systems, and that messages and signals between external interfaces function correctly. Consideration should also be given to any possible adverse effects on the system caused by the sharing of resources, such as power supplies, cabling, physical structures (towers and masts), equipment rooms and containment, with other systems.

Details of interconnections and cause and effect between systems should be documented and detailed on network diagrams if necessary. Where resources are shared, risks to the effectiveness of the system should be assessed and either mitigated by design or be identified to the customer and documented in the SDS.

7.24 Audio

Installed audio must be clearly audible without undue distortion and within the area of coverage of the relevant detectors/cameras as indicated in the system design.

The operation and purpose of audio systems and any cause and effect should be detailed in the SDS.

7.25 Control rooms and 7.26 Operator workstations

Where there is a requirement for live viewing, camera control or system management tasks, a control room must be specified to house these functions.

A 'control room' can be a single workstation or a large operations centre.

Control room design is a specialist area where layouts of displays and control equipment and operator workload and tasking have to be taken into consideration to ensure the effective and safe operation of the system. However, in small systems there may only be one workstation required for controlling cameras or carrying out data processing tasks.

The number of camera views presented to an operator must be decided in the system design phase.

Images must be presented to the operator at a size sufficient to allow them to undertake the viewing tasks.

The operator must be positioned so that they are able to view the information on the display clearly.

Workstations must be suitably protected from unauthorised use, either by physical or application access control.

Where you are responsible for the provision of workstations where operators are expected to spend any significant amount of time, the needs of the operator should be considered and a solution that allows the UR to be met and meets health and safety requirements for display screen equipment should be provided.

Your attention is drawn to The Health and Safety (Display Screen Equipment) Regulations 1992.

7.27 Cabling and 7.28 Supporting structures

Where risks of mechanical damage are identified, cables must be protected by the use suitable conduit, trunking or armour.

Where specific risks of malicious damage are identified in the UR, cables must be protected by suitable means.

Cables types selected must meet manufacturer's recommendations and be suitable for the environment in which they are installed.

Where masts, towers, brackets and supports are used to mount system components, these must be capable of supporting the weight of the component plus any cabling and remain stable and secure during expected climactic conditions (wind and snow).

Where existing support structures are going to be used within the system design these should be assessed to ensure they will be suitable.

You should include in the SDS details of any cabling and support structures (masts, towers and bracket) to be supplied as part of the design. Where existing structures are to be used, this should be stated in the SDS.

7.29 Training

The SDS must include details of the training to be provided, who is to receive the training and when.

Training should be appropriate to the individual or group under instruction.

7.30 Maintenance

An assessment of the type and frequency of preventive maintenance must be included in the SDS to take into account installer and manufacturer's recommendations and any specific environmental or operational considerations.

An assessment of the ongoing requirements to maintain the integrity of the system's network security must be carried out and documented in the SDS.

Maintenance should be a holistic process and recommendations provided in the SDS should cover all system functions and equipment, including updating the firmware and software of system components, applications and operating systems.

8 Installation

Additional requirements have been included in NCP 104 to account for the increased use of shared networks and structured cabling.

Prior to installation, the risk assessment, site survey and system design should be validated to ensure that any changes that may have occurred in the environment will not affect the ability of the system to meet the UR.

Where changes are identified that will or may affect the system design, these should be discussed with the customer at the earliest opportunity and any changes must be documented in the SDS.

8.2 Access to shared networks

Permission must be gained from the customer/system owner prior to the connection of any external devices, such as laptops and memory sticks, to shared networks.

Where relevant, external devices must either have the latest anti-virus software and updates loaded or have been scanned using the latest anti-virus software.

System owners may have processes and requirements in place for the connection of external computers or other devices to shared networks. However, in all cases permission must be gained from the system owner prior to making any connection.

Ensuring that your equipment and devices connected to the shared network are updated, patched and have the latest anti-virus software will also reduce the risk that these may be compromised.

8.5 Cable installation

Where you are responsible for the installation of the network, data cabling must at a minimum be tested for the correct wire mapping (including split pairs), short and open circuits, cross talk, attenuation and speed. The results of this testing must be documented.

Cables, connectors, patch panels, termination blocks and outlet sockets must be compatible, i.e., Cat 5e and Cat 6 components and cables should not be mixed.

Network interconnections over 5m in length should be made using non-stranded (solid) conductors.

Network devices should be connected to interconnections via patch panels or outlet sockets using stranded pre-terminated patch cables.

Network issues may not manifest until sometime after the handover of the system has taken place. Additional network loading, changes to system components during maintenance or upgrades and cable faults caused by the use of the incompatible connectors and poor quality

cabling can contribute to network failures or performance issues. Therefore, it is important that structured cabling is correctly specified, installed and tested.

You are reminded that all cabling should be installed in accordance with the latest edition of the IET Wiring Regulations (BS 7671).

9 Test, commission & handover

As part of the commissioning and handover process, an acceptance test of the system must be carried out.

The work associated with the testing, commissioning and handover of systems will depend on the size and complexity of the system. For a small system, this may be carried out as a single activity. For very complex systems, there may be a need to carry out factory and system acceptance testing before commissioning can be undertaken.

9.1 Test

A system test, using a test plan developed as part of the UR/SDS and agreed with the customer, must be conducted to ensure that all expected functions and features of the system meet the UR and SDS.

Legislative requirements that affect the design of the system must be tested/assessed for compliance.

The test plan should include an assessment of those areas in system design that have been implemented to meet a legal requirement; for example, automatic management of file retention or masking settings on cameras.

Testing should also determine whether default options on system components, which may cause data protection breaches, such as audio settings on cameras, have been correctly configured.

9.2 Commissioning

A formal commissioning process must include a demonstration of the capability of all system components to the customer to enable a decision to be made on the ability of the system to meet the UR/SDS.

Additionally, a physical inspection must be carried out to check the security and correct installation of all system components (including system interconnections).

Commissioning of the system should assure the customer that all functions of the system meet the UR (this can be demonstrated during testing of the system) and that the installation is sound.

At a minimum, commissioning documentation must consist of a copy of the agreed test plan, copies of test results (reference images must be provided to the customer (see 10.1)) signed off by the customer and a completed copy of NCP 104 Appendix D or similar.

9.3 Handover and 9.4 System security

A formal handover of the system must be carried out with the customer/customer's representative present.

Operator training must be carried out as agreed with the customer.

Unless otherwise agreed in writing with the customer, all system accounts used by you must be deleted or locked and the user advised to change passwords when the system is handed over. This includes removing remote access rights to the system.

At a minimum handover documentation must consist of a signed copy of NCP 104 Appendix E or similar (see 10.1).

10 Documentation

All documentary requirements are listed in NCP 104 sub-clauses **10.1 Customer documentation** and **10.2 Installer documentation**.

It is also recommended that a full configuration record of the systems' hardware, firmware and software settings and revisions should be kept for future reference.

11 Maintenance

Additional requirements have been included to account for the increased use of networks. The requirements to access shared networks in sub-clause **11.2** during maintenance activities are the same as sub-clause **8.2 Access to shared networks**.

Additionally, consideration should be given to the need to upgrade or patch system firmware and software during preventive maintenance visits.

*These requirements should have been identified in sub-clause **7.30 Maintenance** in the SDS.*

Appendix G Preventive maintenance report contains the minimum requirements for a preventive maintenance schedule.

Appendices

There are a number of appendices to the main body of the document. These are a mixture of normative documents (requirements that you must follow) and informative documents (guidance and recommendations).

Appendix A Sample risk assessment (informative)

Appendix A contains a suggested format for a risk assessment.

Appendix B Site survey (informative)

Appendix B contains a suggested format for a site survey.

Appendix C Technical description of image categories (normative)

Appendix C lists the various image categories that must be used when specifying what level of detail is required to be captured in each target area in the UR.

This, together with any other factors such as target speed, becomes the basis for camera selection and configuration.

It is recommended that you provide this information to the customer prior to developing the UR.

Table 1 lists typical image heights in percentage figures for common screen resolutions.

This information is included for guidance only and designers should be careful not to assume that by meeting these guidelines they will automatically achieve the level of detail required in the UR.

Appendix D Physical commissioning checks (normative)

*Appendix D lists the minimum requirements (listed under the column headed '**Physical checks**') to be met when checking the mechanical aspects of the installed system during commissioning.*

There is no requirement to modify company documentation to this specific format.

Appendix E Handover & acceptance certificate (normative)

*Appendix E lists the minimum requirements (listed under the columns headed '**Security company handover checklist**' & '**Customer acceptance certificate**') to be met when handing the system over to the customer/user.*

There is no requirement to modify company documentation to this specific format and handover and acceptance documentation may be provided on separate forms.

Appendix F Corrective maintenance (informative)

Appendix F contains a sample corrective maintenance form. This is provided for guidance only.

There is no requirement to modify company documentation to the content or format of this document.

Appendix G Preventive maintenance (normative)

*Appendix G contains the minimum requirements (listed under the column headed '**Check**') to be met when carrying out preventive maintenance.*

There is no requirement to modify company documentation to this specific format.