NCP 104 Issue 3

Security.Improved

Matthew Holliday
Technical Manager (Standards)
NSI Summit 21st March 2019

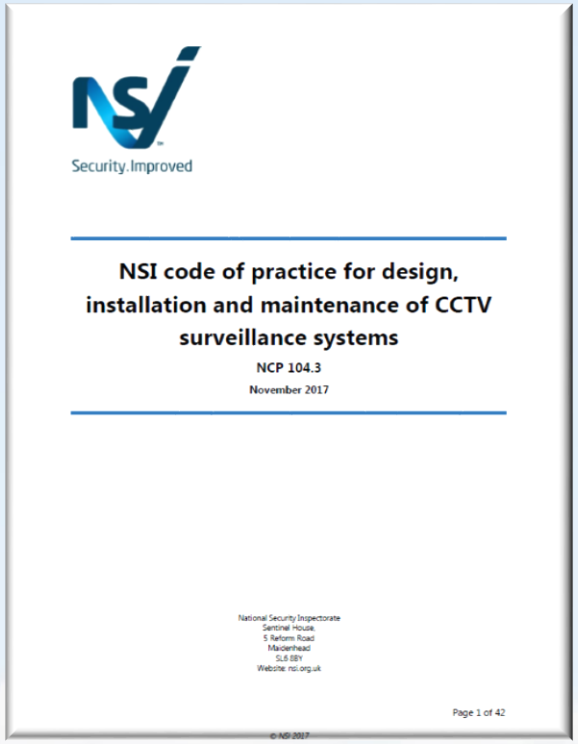
Introduction - Learning Outcomes

- Gain an understanding of the new structure of NCP 104 issue 3
- Gain an understanding of the overall process from site survey to handover
- Understand the timeline for the requirement to implement issue 3

Introduction – Code of Practice

- **NSI code of practice for design, installation and maintenance of CCTV surveillance systems Issue 3**
- Why the need for change
  - Standard update
    - BS EN 50132-7 to BS EN 62676-4

Speakers Notes:
NCP 104 Issue 2 was based on BS EN 50132-7 and is now withdrawn.
In line with the Dresden agreement, International Electrotechnical Commission (IEC) took active control of this standard and subsequently carried out a full revision, as with all IEC standards Cenelec the European Committee for Electrotechnical Standardisation and the BSI then produced its own copy version BS EN 62676-4:2015.



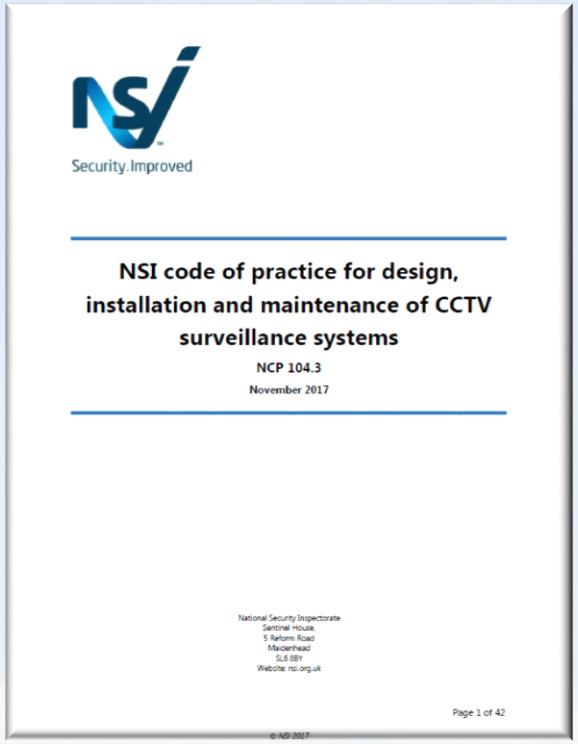
  - Technology updates
    - Analogue to Digital
    - Closed Circuit to Networks (Open and closed)

Speakers Notes:
Changes in technology have been addressed, resulting in changes in terminology. Catering for the move towards digital imaging, including IP network cameras and network storage/transmission.
As we are all aware network security is now a real issue, and must be appropriately considered and mitigated.

Introduction – Code of Practice

- Process update

Speakers Notes:
NCP 104 issue 3 is process based following the process laid out in BS EN 62676-4. SITE SURVEY, RISK ASSESSMENT, USER REQUIREMENT, DESIGN, INSTALL, TEST, COMMISSION, HANDOVER, And finally ongoing Maintenance. With an emphasis on the User requirements, which in other instances is often referred to as an OR - Operational requirement.



- Clarity

Speakers Notes:
In an attempt to avoid ambiguity, references to clauses of BS EN 62676-4 are included, this should provide clarity

- BS 8418 systems are out of scope

Speakers Notes:
Detector activated CCTV systems are not covered by this code of practice, (BS 8418).

Process Update

Speakers Notes:
Issue 3 of NCP 104 leads you through a process

- Risk assessment

Speakers Notes:
In issue 2 of NCP 104 risk assessment and site survey requirements were not included in any detail.

- Site survey
- User requirement
  - Customer engagement
  - Expectation management

Speakers Notes:
The term OR or Operational Requirements is a commonly used term, but may be miss understood by your customers. So the name used in this code of practice is UR User Requirements, this is to focus the attention on engaging with the system user, and finding out what their needs and wants are, along with the findings of the risk assessment. The end user may provide this, or the maintainer may have to draw it up whilst in discussion with the end user.

It is worth noting that the decision to install a CCTV surveillance system to address a particular need, may not be the best option and you should advise the customer what the best solution may be, which might not be a CCTV system where it is unlikely to achieve the users requirements or provide value for money.

Process Update

- System Design

Speakers Notes:

Careful consideration should be given to system design to ensure the UR is met and system performance will be as expected.

- Installation

Speakers Notes:

Covers cable installation and testing, network security, power requirements etc.

- Test, Commission, Handover

Speakers Notes:

The test process must be agreed with the customer as part of the System design Specification (SDS).

- Maintenance
  - Preventative
  - Corrective

Speakers Notes:

Although these requirements may seem onerous, it is intended to be scalable, where the overhead should be appropriate to the size and complexity of the system

Risk Assessment, Site Survey, User requirements

Security.Improved

Risk Assessment

Target
Location
Occupancy
Local Criminality

Speakers Notes:

This may be performed by the customer, but the installer/maintainer can carry it out as part of a single visit, incorporating the risk assessment site survey and UR, however it may need a number of visits and all, some or none of the information may be provided by the user or their representative.

You might want to validate this information before putting your fingers on the keyboard! Remember the quality of this stage can pay dividends should you end up in dispute after installation.

Risk Assessment, Site Survey, User requirements

Risk Assessment

Site Survey

Date, time, location
Drawing, Photograph or Notes
Distances
Equipment Locations
Illumination
Environment
Restricted access, Civil works

Speakers Notes:
This may be carried after the UR.

Risk Assessment, Site Survey, User requirements

Security.Improved

Risk Assessment

Site Survey

User Requirement

Speakers Notes:
This should be drawn up by the user or by the installer/maintainer whilst in discussion with the user. As the test plan is based on the UR consideration must also be given to how this will be developed and conducted. Perhaps an accurate pixel per metre measurement or test for the most critical security installations. For simple systems when these processes are complete you will probably be in a position to provide a quote or estimate for a system design. The full system design need not be completed until the contract has been awarded unless the client specifically wants one.

Basic Objectives
Surveillance Areas
Activity to be Captured
System performance
Operational periods
Environmental
Resilience
Monitoring Recording
Export
Operators
Training
System Expansion
Audio
Limitations

Design

Speakers Notes:

The system design must address all the requirements captured in the UR, and take into account any constraints imposed by limitations identified in the site survey and or the limitations of any users.
All limitations identified must be discussed with the customer and documented.

When translating the UR into a system design requirements in the following areas must be considered and documented where necessary, The system design must be fully documented.
There are Eight design areas:

Data protection
Protection of Freedom
Private Security industry
Town & Country planning
Clear Neighbourhoods and Environment

Security.Improved

Design

Legislation

Site Plan

A site Plan must be included
CAD
Or
Sketch
Or
Description

Design

Legislation

Site Plan

Imaging and sensing

Camera equipment
Functional cameras
Field of view/object size
Detectors, video analysis, alerts and thermal imaging
Illumination

Security.Improved

Design

Legislation

Site Plan

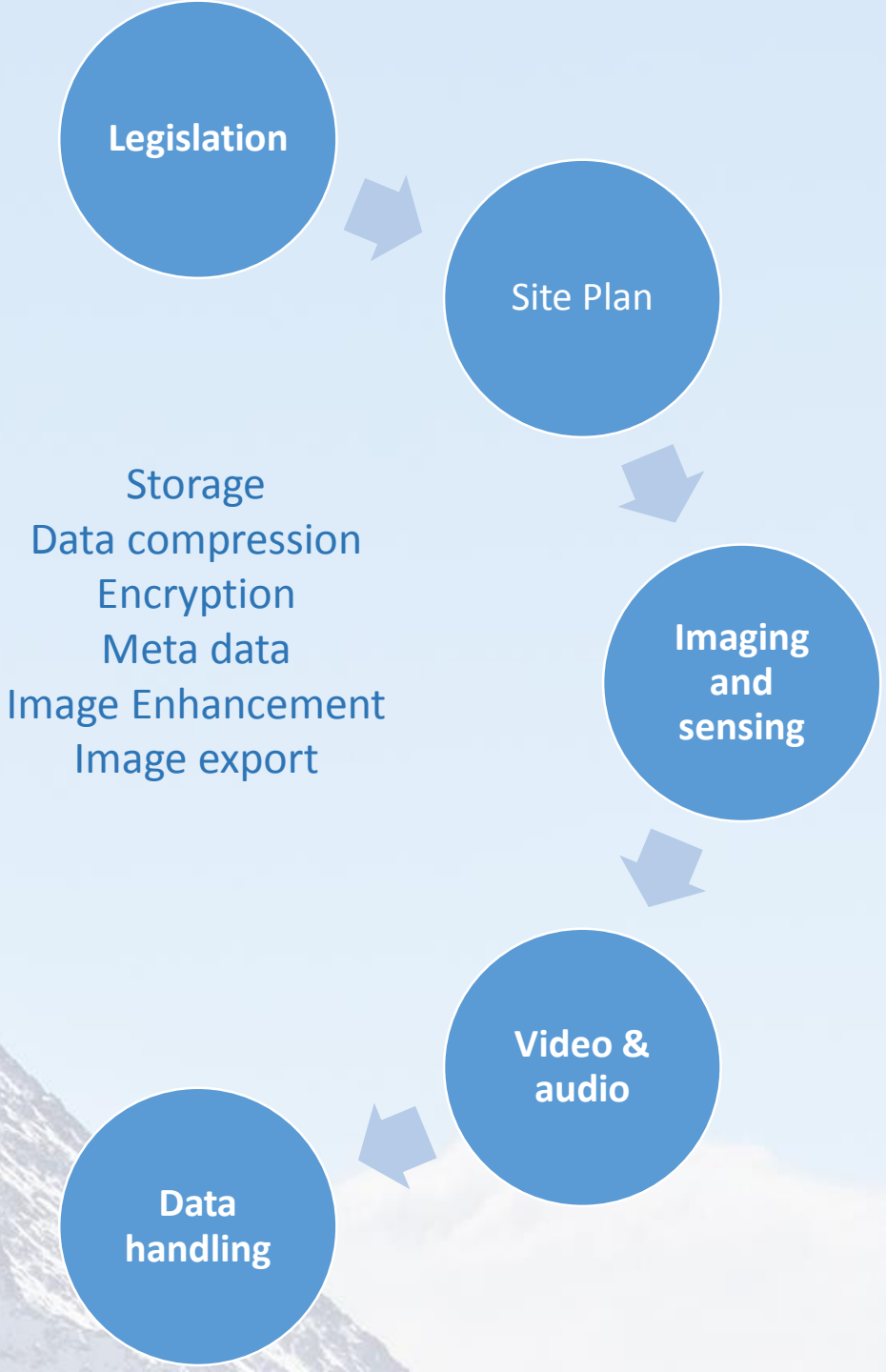
Video/audio performance
Video frame rate
Video resolution
Audio

Imaging and sensing

Video & audio

Security.Improved

Design



Security.Improved

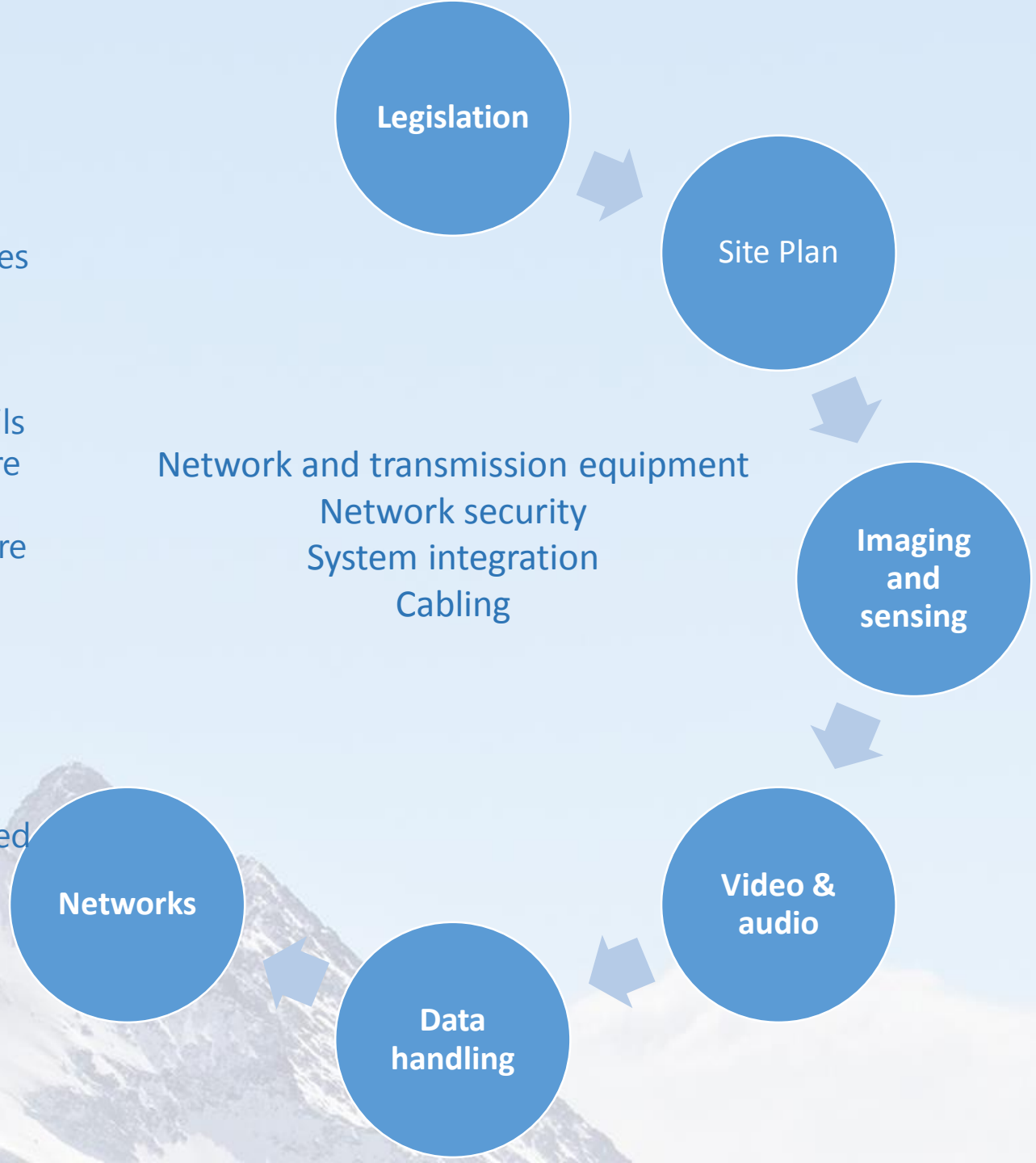
Design

Speakers Notes:

Constraints on connecting devices to a users network in terms of affecting bandwidth and introducing vulnerabilities. You have to assess and provide details of the bandwidth needs if you are connecting to or are using user provided infrastructure and/or are connecting to the Internet.

Vulnerabilities on networks and interconnections to external networks provided by you.

You and probably your client need to be assured that whatever you install can be suitably hardened against malicious attacks on the networks.



Security.Improved

Design

Security.Improved

Design

Security.Improved

Install

- Validate design prior to starting

Speakers Notes:
Has anything changed, is the design still valid?

- Changes to be documented and agreed

Speakers Notes:
If you have to change the design? Document it

- Ask permission to connect diagnostic tools to user provided networks
  - Software and firmware at latest agreed revisions

Speakers Notes:
Ask the person who is responsible for the security of any shared network,
The company may have an IT policy that could impact on your activities, e.g. software release policies etc..
Equipment firmware and software can have vulnerabilities leaving a risk to network security, so the latest official versions should be loaded and or installed..

- Test structured network cabling and infrastructure

Speakers Notes:
New skills needed?, Structured network infrastructure requires new skills, Wire map testing, including cable length validation and where required cross talk and latency

Test, Commission, Handover & Documentation

- Test plan based on UR agreed with customer

Speakers Notes:
A test plan can be subjective (walk test, image recognition) or objective (measurement of image quality) or a mixture of both but must be carried out in the expected illumination over the whole period that the system is designed to operate.

- Commissioning to demonstrate functional capability and assure system security and installation quality

Speakers Notes:
Appendix D contains an example commissioning checklist for physical aspects, but not for functionality. A functional check list will have to be developed for each system.

Does every thing work as designed; can you see what you need to see when you need to see it.
will there be enough storage capacity,
do the exported images meet the users requirements,
do triggers and alerts operate correctly,
when the network is fully loaded is there any image degradation,

Test, Commission, Handover & Documentation

- Cyber secure
  - Agreement for holding passwords
- Carry out operator training
- Customer documentation provided

Speakers Notes:

have all security patches and updates been applied, can you remotely access the system if necessary, are unauthorised individuals prevented from doing so,

are all access and authentication measures in place, have you checked and tested them? Do you need to carry out any form of cyber penetration (pen) test??

Delete all unused passwords and open ports. Unless agreed with the customer delete passwords used during commissioning.

Agree who holds and has responsibility for passwords? and how they will be managed

Maintenance

- Competent staff
  - Corrective
  - Preventative
    - Schedule of maintenance
    - Requirements identified in 7.30 of SDS

Speakers Notes:
Engineers Maintaining must have the appropriate skill sets and be competent to carry out all corrective and preventative maintenance tasks
Maintenances should be performed in line with an agreed schedule.
There is a list of checks to be carried out on a preventative maintenance, Annex G provides an example checklist.
Annex F provides an example check list for corrective maintenance.
Ensure that any schedule for maintenance as agreed in the SDS is met in full

- Permission to connect to networks

Speakers Notes:
Remember to ask permission before connecting test devices e.g. laptops to customer networks.

Maintenance

- Include system software and firmware updates, if necessary

Speakers Notes:
OS patches and software security updates will need to be updated as required.

- May need process to include the management of ‘critical’ updates

Speakers Notes:
To help avoid cyber security risks, Unplanned critical updates should be considered outside the normal preventative maintenance schedule.

Security.Improved

www.nsi.org.uk/companyfinder