National Protective Security Authority

User Guide on Automatic Access Control Systems

(EIS0002)

Disclaimer

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Contents

1 Introduction

1.1 What are Automatic Access Control Systems?

Automatic Access Control Systems (AACS) refer to the equipment used to control the passage of people and vehicles into and out of protected areas and premises. Access control is about managing 'who can go where and when'.

Manual access control measures (barriers, structures, portals, locks and guards) are integrated with automatic access control systems to provide functionality such as automated identification/authentication, audit information and zone-controlled access.

This document provides high-level guidance on AACS and is divided in the following sections:

1. Introduction
2. About AACS
3. Selection
4. Installation
5. Commissioning
6. Management
7. Maintenance

Authentication may be achieved by any of the following three metrics:

Something we know

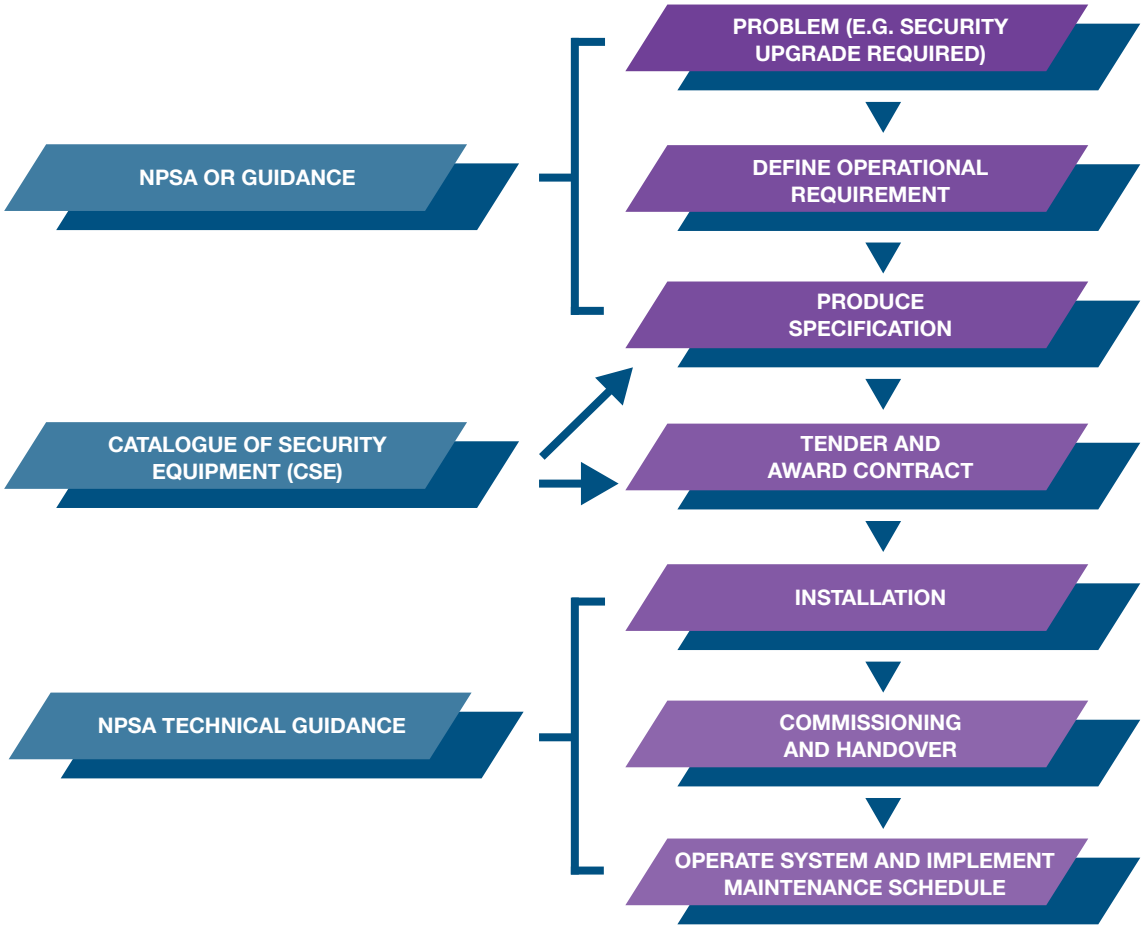
Something we are

Something we have

1.2 Steps for Deployment

The successful specification of any security system, including AACS, is dependent upon the development of detailed Operational Requirements (OR).

The following diagram illustrates the stages prior to the deployment of a system.



2 About AACS

2.1 Components

An AACS may be considered as comprising a number of separate but integrated components.

For an AACS to be effective, all its components must be of the correct standard and integrate together. The table below shows some of the components which may be used to protect a secure area with two portals providing access.

Components	*Description*
Keypads & Readers	Means to input user credentials, e.g. PIN, Token or Biometric, for authentication by the controller.
Portal	Controls access to the protected area by receiving release commands from the controller. Anti-tailgate measures, portal type and construction/ type of release mechanism to be considered. Could be a door, tubestyle, turnstyle or other product.
Controller	Manages the operation of the AACS to predefined rules, performs authentication, portal release and the processing of AACS alarms. The hierarchy of operation and location of the controller must be considered.
Database	Holds user information and system transactions. May be held locally within a controller, centralised or distributed. Security and resilience of the database to be considered.
Network topology	May be stand-alone or use a shared LAN.
Power supplies	May be integral to other components of the AACS or separate. These must have sufficient capacity to supply the load placed upon them and have sufficient reserve capacity to ensure that the system continues to run in the event of a power failure.
Policy	Covers rule-base, time/area definition and database management and should be considered before writing the Operational Requirement.
Procedures & instructions	Must be site specific, i.e. the installer should supply information regarding the specific use of the system for your site. This should be supplemented with site management procedures written by site management for specific events.

2.2 Advantages and Disadvantages

2.2.1 Advantages

- AACS are permanent and continue to provide control of entry even in the temporary absence of guards, although they should not be considered as a total replacement for security personnel where their use is considered appropriate
- They are automatic systems; cannot be distracted, suborned, persuaded or threatened
- The initial capital expenditure (excluding on-going maintenance costs) is a one-off outlay as distinct from the recurring costs of guards
- They are programmed to detect the attempted use of passes (tokens/cards) which have been deactivated after being reported as lost or stolen
- They enable authorised users to indicate that they are being forced to enter under duress if such functionality is desirable
- An audit trail is provided of events and actions
- Zoning of areas is possible allowing higher/selective security
- Alarms are provided for selected actions/events e.g. door left open too long
- Tokens can be programmed with an automatic expiry date/time

2.2.2 Disadvantages

- AACS require human intervention to deal with visitors, deliveries, breakdown of the system and emergencies
- They alone cannot prevent the entry of an unauthorised person in collusion with an authorised person
- The concept and layout of an AACS together with the measures to control entry and exit may cause some inconvenience to legitimate users causing increased effort and delay
- There is a significant commissioning and operating overhead

- AACS need regular and continuing maintenance. Service procedures for a satisfactory system maintenance agreement need clear definition of the actions required on system breakdown or failure

- Excessive reliance and/or confidence in the system can cause faults or system alerts to be ignored by operators, especially where such alarm events are regular occurrences and operators have become used to ignoring them

2.2.3 Considerations

- System administrators such as security officers or pass office staff need to be fully aware of their role and how to operate the system, in particular for more complex technical equipment

- Adequate ongoing system training should be given to both operating and management staff to ensure that they remain conversant with system, operational and management procedures

- The implementation of an AACS may require higher IT skill levels, reflecting the increased complexity of the system

3 Selection

3.1 Factors

Several factors play a role in determining the suitability and design of an AACS for a site. They relate to the operational requirements as well as the local circumstances in which the AACS will operate. Before attempting to write a performance specification for an AACS, it is imperative to ensure that a detailed operational requirement (OR) has been produced. Considerations when creating an OR can be seen below.

Environment

Consider the activities undertaken at the site/building

Define the threat

What specific assets require protection?

Are there any special features that need to be accounted for? e.g. listed building status

Internal conditions need to be considered: humidity, temperature and atmospheric contamination

Deployment

Consider the requirements for the AACS

What level of protection is required?

What control restrictions will be included? e.g. anti-passback, zoning, etc.

To which user groups should the control of access be applied to?

For AACS being installed on existing sites it is important to identify what existing measures will remain when the AACS is deployed

Integration

Consider whether the AACS will work in conjunction with other components such as intruder detection or video surveillance systems

What other types of equipment and systems are planned or in use?

Who will be responsible for the integration?

How will the system integrate with the overall security strategy?

Response

Consider how and where a response will be initiated from

Will the systems be monitored from an onsite control room or remotely?

Is there a permanent presence of security personnel onsite as well as the AACS?

Outline the responses to certain circumstances e.g. anti-passback reset following network failure, system failure or evacuation due to fire alarm

Regulations

Consider any regulations the AACS will have to adhere to

Equality act 2010

Requirements of network design

Ensure the AACS strategy is coordinated with fire regulations and emergency exit requirements

General Data Protection Regulation (GDPR)

3.2 Design Features

ZONING

- The system can provide area/time zoning control functions where the system will allow or disallow entry/exit. They can be used to prevent entry or to generate alarms if a user is within a secured area outside a permitted time

ANTI-TAILGATING

- Prevents two people from passing through an access control portal using only one access control credential

ANTI-PASSBACK

- Anti-passback can be used to stop a single token being used to make multiple access attempts without exiting
- To prevent 'passback' the system must not let a token be used to gain access more than once without the token and owner being registered as having left the area
- For a fully secure system, anti-passback and anti-tailgating should be combined to prevent both multiple uses of a credential to enter without exit and multiple entries on a single credential

FAIL SAFE/FAIL SECURE

- All buildings must comply with fire regulations and emergency exit requirements. Where there is a requirement for means-of-escape it should not rely on the operation of the AACS
- Subject to the specific operational requirements, in the event of a power outage, the AACS system can provide for 'fail safe' or 'fail secure' modes of operation. In fail safe mode portals will release on system failure; in fail secure mode portals will remain closed

SYSTEM DATABASE

- AACS can store their data in a number of locations within the secure area. The databases should be configured to ensure that they are secure and up to date. Internal or external cyber penetration testing during commission is recommended.
- Any back-up copies should be afforded protection commensurate with the information contained within them. This applies to their storage and their movement
- The control of the data records must meet the requirements of the Data Protection Act

UNINTERRUPTED POWER SUPPLY

- Any AACS will require that provision be made to allow operation to continue in the event of a mains failure until support can be deployed to the site
- The minimum time should be determined by the operational requirement

USER INTERFACES

- Audible and visible cues should be used at the reader head to enable users to interact with the system but their function should not compromise security, for example - 'entry failed' should be indicated, rather than 'valid card, but incorrect PIN
- Duress PINS can be used in conjunction with a clear procedure and a defined and communicated response. Users must know what will happen if they enter the duress PIN
- Keypads and readers should be positioned to avoid oversight by any unauthorised persons
- The requirements of the Equality Act in relation to the AACS must be met

3.3 Network Security

The threat from external compromise is of particular concern where IP connected security systems are deployed. The threat can be both to the security system directly or from an attacker using the security system to penetrate other IT, or vice versa.

NPSA recommends that the AACS be segregated from other IT systems wherever possible. However, it may be necessary to have the AACS on a shared network. NPSA would suggest that the AACS also holds the CAPSS (cyber assurance of physical security systems) accreditation.

CAPSS is mandatory for AACS systems seeking to achieve higher NPSA grades in an NPSA product evaluation.

For further information on CAPSS please visit https://www.npsa.gov.uk/cyber-assurance-physical-security-systems-capss

4 Installation

The AACS should be installed according to the manufacturer's installation procedures. If these are not followed, difficulties in determining liability could arise should the AACS fail to perform as expected.

The following are some significant design requirements that should be considered:

- The mounting location of controllers, power supplies and, where applicable, network equipment: these must be located within the protected area, minimising the possibility of accidental damage or deliberate attack. Careful consideration must be given to cables and junction boxes connected to the portal release mechanism and/or activation equipment when fitted to or near the portal.

- Future site expansion: provision should be made for potential expansion plans at the site. The security of additional components must meet that of the installed AACS.

- Environment: while this will be critical for components installed outside buildings, internal conditions may also need to be considered including, humidity, temperature, and atmospheric contamination. The installer/specifier should be informed of any specific environmental issues, for example if the equipment is to be located within noisy or high vibration areas.

5 Commissioning

Following installation, the AACS should be subjected to a range of commissioning tests. Commissioning tests assess the functionality and performance of an AACS to ensure it has been installed to, and performs in accordance with, the required specification. If the AACS does not fulfil the stated performance, the installation can be rejected. Contracts placed for AACS must state that commissioning tests will be performed prior to acceptance of the system.

5.1 Considerations

- Commissioning tests provide performance data from which any future deterioration can be measured, and hence remedial action justified. If adjustments are made to the AACS - either as a result of initial commissioning tests or for any other reason - the tests would need to be repeated.

- The installation contractor may conduct a site acceptance test (SAT) following system installation. This comprises a structured demonstration of all system functions to show that it is performing to specification. This should not preclude the end user from conducting independent commissioning of the new system to ascertain the system's performance.

- A commissioning test plan should be devised to assess performance in relation to the defined operation. The amount of time required for commissioning will vary depending on the size and complexity of the system and can range from a few hours to several days. It should not be assumed that a successful outcome on one portal is indicative that all other portals will respond correctly. The complex nature of AACS means that many of these systems will need to be programmed individually for each device or portal connected to it and the chance or error is proportionate to the size of the system. Therefore, all tests should be applied to every portal and device as appropriate.

- Where AACS are installed as part of an integrated security system (for example with an existing alarm management system or video surveillance system) it should be tested as a whole. This will ensure that the AACS operates effectively as part of the integrated system. When undertaking commissioning tests it is essential to have good communication with the control room. This ensures that the control room is able to confirm if an alarm or other event is received. It will also allow them to check whether the tests have generated any unexpected/spurious alarms.

- Commissioning tests should not only test AACS performance but should also test any other required functionality tests. This should include removing power to the system to certify that the uninterruptible power supply works as required; or that the AACS fails safe or fails secure depending on the requirement given in the specification.

- Results of the commissioning tests should be used to determine whether the AACS meets the specification and should therefore be accepted.

5.2 Documentation

On acceptance and handover of an AACS, drawings and manuals covering the installation, operation and maintenance must be provided to the person responsible for maintaining and operating the system.

Commissioning documentation should include but, not be limited to, the following information:

- A DESCRIPTION OF THE MANNER AND LIMITATIONS OF OPERATION
- PROOF OF COMPLIANCE WITH RELEVANT STANDARDS OR SCHEMES
- SET-UP/ TIME PARAMETERS
- INSTRUCTIONS FOR THE SWITCHING ON, OPERATION, SWITCHING OFF AND ISOLATION OF THE SYSTEM
- INSTRUCTIONS FOR DEALING WITH EMERGENCY CONDITIONS
- INSTRUCTIONS FOR SYSTEM MAINTENANCE
- A LIST OF APPROVED SUPPLIERS, INSTALLERS AND MAINTAINERS
- DRAWINGS INCLUDING DIAGRAMS AND SCHEDULES SO THAT THE SYSTEM CAN BE SAFELY OPERATED, MAINTAINED, INSPECTED AND TESTED
- DRAWINGS SHOWING THE PHYSICAL ARRANGEMENTS TO ASSIST THE LOCATION AND IDENTIFICATION OF ALL COMPONENTS

6 Management

Once a new AACS has been procured, installed and commissioned, it is important to establish good working practices to ensure the system effectiveness in the long-term. Good working practices include, but are not limited to:

6.1 Privilege Management Policy

A comprehensive privilege management policy should exist that appropriately secures privileged accounts and enforces organisational policies for privileged account use.

The authority granted to particular users and administrators responsible for an AACS should reflect their specific needs. User accounts shall be based on the principle of least privilege (PoLP), enforcing the minimal level of user rights, or lowest clearance level, that allows users to perform their role.

The AACS deployment shall have clearly defined separation of privileges and separation of duties. In practice it is recognised that an individual may have multiple responsibilities but under no circumstances should a ‘super-user’ be created who has full unrestricted access to the system. Monitoring, auditing, and authentication controls should combine to prevent unauthorised access to, and allow the rapid detection of unapproved use, of privileged accounts.

Access Level Examples

User Type	***Functionality***
Level 4 User e.g. Administrator	Database / Configuration files / Creation of configuration device / programming terminal / Back-up / Log in engineers / View all logs / Connection of external devices / media / software updates / Disable & inhibit 'Request-to-exit' buttons
Level 3 User e.g. Supervisor	Log in engineers / Operational configuration files / Alert suppression / Area de-activation / Temporary revocation rights / Issue temporary passes / View guard logs / View event logs / View / print roll call of areas / System status
Level 2 User e.g. Guard	Accept & re-set alarm / View alarm logs / Incident logs / System status
Level 1 User e.g. Enrolment Officer	Enrol & revoke users / Assignment of user profiles / PIN control / Production of passes
Guest User 2 e.g. Engineer*	Error logs / Network configuration
Guest User 1 e.g. Remote Engineer*	View error logs / Fault data

* Guest users such as Engineer log-on requires administrator or supervisor authentication. Engineering personnel should never be able to access the AACS database or any enrolment officer capabilities/configuration files unless it is under the direct supervision of a Level 4 user administrator.

6.2 Operation

User Interface

- Must be clear, displaying relevant information to the operator. It should assist the operator in their decision-making process, enabling the appropriate response to be deployed.
- The use of multiple sensory indicators (audio, visual) should be considered to ensure a timely response to alerts

Alerts and Audit Logs

- AACS generate alerts and audit logs. Security Officers should respond to alerts using standard operating procedures
- Tamper alarms should always be investigated and their cause determined
- Audit logs should be reviewed and actioned by the supervisor
- Audit logs can also record details of any changes that are made to the AACS

6.3 Training

A range of training, appropriate to user access level, position and responsibilities will be required. Training should be undertaken by both the system installer and the site management and should cover the duties and responsibilities for:

- System administration, security officers, operators, supervisors and managers
- System users – including as a minimum:
  - The use and security of tokens
  - Policy regarding PINs
  - Wearing of badges
  - Policy in the event of a lost token
  - Procedures to follow in the event of a system failure
  - Rules for visitors
  - Emergency evacuation procedures
  - Any specific local requirements including duress procedure if enabled.

6.4 Enrolment and Token Issue

A separate work station and reader for enrolment should be setup subject to the level of security required. This should be located within the secure perimeter and be protected physically with controlled access. A clear policy should be defined covering the distribution and control of tokens. In high security environments, PINs should be machine generated and not changed by the user. Prior to enrolment the applicant's identity must be verified through a pre-employment screening process. A further identity check should be made at the point of card issue.

An overview of the procedures to follow for the enrolment and token issue of varied user groups is provided in this diagram:

Permanent Staff and Permanent Contractors

- ID verification
- Tokens set to expire on a suitable date
- Only issued to the owner
- Third party collection not permitted

Contractors (Non-permanent)

- Treated as either escorted or unescorted visitors dependent upon the level of assurance/trust

Escorted Visitors

- Nominated host and prior appointment
- ID verification
- Not issued with an AACS token
- Issued with an identification or an escorted visitor pass

Regular Visitors

- ID verification
- Full background verification of business need and parent organisation affiliation should be conducted
- The parent organisation must agree to inform host organisation of changes to vetting or employment status
- Unescorted Tokens and PINs valid for a fixed period of time

Unescorted Visitors

- Nominated host and prior appointment
- ID verification
- Trusted visitors issued with an unescorted visitor token
- Tokens not in use should have the same protection as active staff tokens
- Tokens expire at the end of the day and be handed in

7 Maintenance

To ensure that the installed AACS continues to operate as required it is important that a comprehensive maintenance programme is followed. The maintenance schedule should include selected tasks to check that the operational requirement is still applicable and determine whether there have been any changes during the life of the AACS that may have affected its operation and performance.

Maintenance must be undertaken using suitably approved and security cleared staff. Access by engineers must require that they first be granted access by an administrator or supervisor before being able to use their own engineering log-ons. Any device used to maintain the system (programming terminals, laptops) should remain on site and be appropriately protected.

The installer must provide the maintenance requirements of the proposed AACS. It is imperative that the maintenance regime and any maintenance contractors are approved by the supplier to ensure the supplier can be held accountable for any failure of the AACS to maintain the required performance. Operators should be aware who has the authority to call out the maintenance team if a problem arises and what the response time should be.

Following any maintenance, repairs, upgrades or adjustments, the AACS should be retested to ensure that it continues to operate as required in the specification.

The maintenance log book must be kept up to date. It should include details of maintenance tasks carried out along with the corresponding test results. The maintenance log should also contain a copy of the commissioning test results which can be used for comparison with any subsequent tests.

Details of all breakdowns, repairs, replacements and system changes should also be recorded.

AACS bridge IT networks, software, applications, electronic devices and locking hardware, as such the maintenance requirements are likely to cover multiple teams with different remits. Maintenance tasks, schedules and activities should cover all of these areas.

8 Summary

This guidance document has provided an overview of Automatic Access Control Systems. The content can be summarised as follows:

Key Points

1. Operational requirements should guide the selection and specification of a AACS
2. AACS have associated strengths and weaknesses
3. AACS features should be researched and selected according to the operational requirements to add value to the basic function of controlling access
4. A specification should comprise detailed information about the required AACS, including details of other systems to be used with the AACS
5. AACS should be installed following the manufacturer's installation procedures
6. Commissioning tests should be conducted upon installation and prior to acceptance
7. Regular maintenance and testing is paramount to ensure the integrity of the AACS

Further Information

Further advice and supporting guidance documents are available through the relevant NPSA adviser, or from the NPSA website **www.npsa.gov.uk.** Further reading is available on the following related subjects:

- NPSA Evaluation Standard for Access Control
- NPSA Guide to Producing Operational Requirements for Security Measures
- NPSA Catalogue of Security Equipment
- Equality Act 2010 - available from gov.uk
- Data Protection Act - available from gov.uk