

TS 2.10.14

GENERIC ELECTRICITY SUBSTATION DESIGN MANUAL

FOR CIVIL, STRUCTURAL AND BUILDING ENGINEERING

SECTION NO : 14

TECHNICAL SECURITY SPECIFICATIONS FOR INTEGRATED SECURITY SOLUTION SITES

This document is for internal and contract specific use only.

Disclaimer

NGG and NGET or their agents, servants or contractors do not accept any liability for any losses arising under or in connection with this information. This limit on liability applies to all and any claims in contract, tort (including negligence), misrepresentation (excluding fraudulent misrepresentation), breach of statutory duty or otherwise. This limit on liability does not exclude or restrict liability where prohibited by the law nor does it supersede the express terms of any related agreements."

TABLE OF CONTENTS

PURPOSE AND SCOPE	2
PART 1 - SITES.....	3
1 SITES GENERAL REQUIREMENTS	3
2 PERIMETER SECURITY	5
3 ID AND ACCESS CONTROL.....	9
4 CCTV.....	11
5 SECURITY LIGHTING	15
6 BUILDING HARDENING	18
7 TUNNEL SECURITY.....	20
8 SITE AUDIO REQUIREMENTS.....	21
9 ISS COMMUNICATION REQUIREMENTS	21
10 ISS POWER AND BACK UP POWER REQUIREMENTS	21
PART 2 – ISS ALARM RECEIVING CENTRE (ARC) AND SITE AMS.....	22
11 THE ARC GENERAL REQUIREMENTS	22
12 MANAGEMENT SUITE	23
13 CCTV.....	24
14 ACCESS CARD MANAGEMENT	24
15 AUDIO SYSTEM	25
16 LIGHTING	25
17 GRAPHICAL USER INTERFACE (GUI)	26
18 SYSTEM ADMINISTRATION.....	26
19 COMMUNICATIONS.....	27
20 PERFORMANCE	27
21 BUSINESS CONTINUITY	28
22 CYBER SECURITY	28
23 ENVIRONMENTAL	29
24 SOFTWARE AND LICENSING.....	29
25 POST DELIVERY.....	29
PART 3 – DEFINITIONS AND DOCUMENT HISTORY.....	30
26 GLOSSARY OF TERMS	30
27 AMENDMENTS RECORD	32
28 IMPLEMENTATION	33
PART 4 – GUIDANCE NOTES AND APPENDICES	33
29 REFERENCES.....	33
APPENDIX A SITE SECURITY PLAN AND KEY MANAGEMENT – DURING CONSTRUCTION	35
APPENDIX B COMMISSIONING AND CAST AUDIT POST CONSTRUCTION	36

PURPOSE AND SCOPE

The purpose of this document is to detail National Grid's technical and procedural requirements for the minimum security requirements on Integrated Security Solution (ISS) designated new and existing operational electricity substations.

This Technical Security Specification (TSS) document has two parts; Part 1 is intended to be the minimum security requirements that shall be deployed and applied to existing sites, new sites, extensions to sites or any other site works on designated Integrated Security Solution (ISS) sites. Part 2 is intended to be the minimum requirements for delivering the ISS signals to the ARC. These will be applicable to all electricity substations that have been designated for the Physical Security Upgrade Programme (PSUP).

The requirements listed below will form the basis of the integrated security solution and where there are several options the individual Site Specific Operational Requirements (SSOR) documents will specify which option to for a specific site. The SSOR can only select from the solutions in the TSS and a Technical Deviation should be sought for any other solution.

The process flow is therefore TSS → SSOR → Front End Engineering Design (FEED) Design Intend Document (DID) → Detailed Design → Design Approval → Design Assurance → Construction.

This document also relates to additional measures that may be required on sites to enable the site to be further secured, such as tunnel security measures where applicable.

TSS Objectives

- To provide minimum standards required for implementing an agreed integrated security solution to ISS designated sites.
- To enable key stakeholders to understand the purpose and requirements of the ISS and the requirements for the successful implementation of the PSUP.

To obtain engagement from the business functions to support the implementation of the programme.

- To ensure the most appropriate value engineered solutions are considered. Where options are given in the TSS, National Grid will retain the right to audit and challenge design decisions made from a value engineering perspective.

To provide temporary Security requirements during construction.

- To provide a document that along with the SSOR can be utilised by the Home Office CAST auditors. These Fit for Purpose (FFP) audits are completed on DECC's instructions at the end of both design and construction phases.
- To provide a document that along with the SSOR can be utilised by the Value for Money (VFM) auditors. These Value for Money (VFM) audits are completed on DECC's instructions at the end of both design and construction phases.
- Critical Assets and Systems will be determined on a site by site basis and identified in the Asset Management Needs Case.

Strategic Intent

The intent of the ISS is to deter, delay, detect and gather evidence of unauthorized access to National Grid sites, forming an integrated physical security solution that is resilient and capable of meeting National Grid's ISS in a cost effective manner ensuring value for money.

- This document refers to: perimeter security, building hardening, CCTV, access control, security lighting, intruder detection systems, audio challenge and IS system that will be integrated on site to enhance security.
- Control of the ISS, management of any alarms generated by the system shall be undertaken by the Alarm Receiving Centre (ARC).
- The ISS installed on site shall be configured such that an alarm will be generated on site when there is an unauthorised attempt to gain access to site, intrusion into site and in the event of power loss / outage on the site.

INFORMATIVE: Various references are made throughout this document to third party standards and guidance documents. Where the particular issue or revision of such documents is not stated, this is intentional and the user of this document shall refer to current issue at the time of use.

PART 1 - SITES

1 SITES GENERAL REQUIREMENTS

1.1 Civil

- 1.1.1 The design life of the fence civil works (including anti burrow cill) shall be partdesigned to meet NG standards.
- 1.1.2 New and existing buildings on ISS sites will require to be assessed on a site specific basis to determine the requirements for hardening to prevent unauthorised access to and protection for Critical Assets and Systems. Existing fire / blast zone ratings shall be maintained as a minimum.
- 1.1.3 All building hardening measures need to be commensurate with the building / room / tunnel fabric and construction.

- 1.1.4 Detailed designs will be required to prove the impact on the structural integrity of any building / room to accommodate any building / room hardening works.
- 1.1.5 CCTV signage to fulfil our obligations under the Data Protection Act 1998 shall be installed on all sites, this will consist of A3 signage on vehicle gates and A4 signage on pedestrian gates, the ARC Contact telephone number displayed shall be 01926 653776.
- 1.1.6 Signage shall be fitted to gates as per National Grid specifications and in accordance with BS 5499 and agreed with the Site Operator. e.g. Emergency exit signage.

1.2 Technical

- 1.2.1 All existing CCTV systems should remain unless they interfere with the new ISS system, if removed the replacement system should ensure camera views and functionality are as previously installed by the Site Operator.
- 1.2.2 External cabinets/panels and internal cabinets/panels that are deemed at risk of temperatures outside those stated in 1.4.2 containing electronic equipment for the ISS shall be fitted with thermostatically controlled anti-condensation heaters. In addition, suitable means shall be provided to ensure the maximum temperature in the cabinet / cubicle does not exceed that recommended by the manufacturer of any equipment contained therein, thus ensuring the correct operation of the system at all times.
- 1.2.3 On all sites the ISS System should provide 2 volt free contacts configured to deliver the following signals;
 - Station PIDS – On (HV for EPID) / Off (LV for EPID)
 - Station PIDS – Alarm / Clear
- 1.2.4 The access control system shall integrate with security physical barrier / fencing, lighting, CCTV and PIDS etc.
- 1.2.5 Interacting with other components of the ISS system the access control system, via the use of ID/ Access cards shall be capable of:
 - a) Being used to control where appropriate the site PID system.
 - b) Being linked to either operational or ISS lighting to illuminate the route to and from the ISS building for personnel entering or leaving site.

1.3 Construction

- 1.3.1 The design and construction of all permanent and temporary works on ISS sites shall comply with National Grid's environmental and sustainability policies. Notwithstanding this, the construction works shall be carried out to minimise waste and maximise recycling of suitable materials.
- 1.3.2 Perimeter security shall comply with local / national planning requirements and local / national environmental requirements.
- 1.3.3 Where appropriate, an optimum 5 metres vegetation free verge from the fence line (external to the site), and a minimum 2 metres shall be maintained. The maximum length of grass at 20 cm and the bottom of the canopy of trees shall be maintained at 3 metres from the ground level. This requirement should be capable of being varied to site specific conditions.
- 1.3.4 Design and installation should follow the ISS Project Generic Design Manual (ISS GDM).
- 1.3.5 The design will consider appropriate flood mitigation techniques as previously used on operational equipment on site e.g. raised electronics for critical equipment. Flood probabilities and depths should be supplied to the contractors ahead of design.
- 1.3.6 The ISS shall take full cognisance of the Process Safety and Operational procedures on all ISS sites and the system shall be designed to maintain emergency requirements including muster, access, egress, fire alarms and relevant business unit procedures.
- 1.3.7 Where the contract works renders existing access / security equipment redundant, this shall be decommissioned, made safe and removed, where practicable, including making good where holes / mountings etc. are removed.

1.4 Environmental

Unless otherwise stated, equipment installed as part of the ISS works on site shall meet a number of environmental requirements which are:

- 1.4.1 The technology components of the delivered ISS solution should be designed for a minimum 15 year supportable lifetime, ensuring sufficient spares, support and availability of equipment throughout this period.
- 1.4.2 Equipment such as, mounting hardware, cabling, LV switchgear, and diesel generators shall be designed for a minimum 40 year supportable lifetime.
- 1.4.3 The ISS system shall function within the following operating temperatures of -10°C to + 55°C; storage temperature of -25°C to + 70°C and humidity of 5% to 95% non-condensation.
- 1.4.4 Components of the system shall be designed to achieve the above requirements without relying on additional mechanically assisted cooling of any kind (e.g. fans) where this is not practicable agreement should be sought from National Grid ISS Assurance Engineer.
- 1.4.5 The equipment shall be able to withstand shock and vibration to BS EN60870-2-2 (class Bm) where this is not practicable agreement should be sought from National Grid ISS Assurance Engineer.
- 1.4.6 External cabinets / equipment shall achieve ingress protection to IP 65 (BS EN 60529) as a minimum standard. External cabinets housing batteries shall achieve IP 55 (BS EN 60529).
- 1.4.7 The equipment shall meet the electromagnetic compatibility standards BS EN 61000-6-2 and BS EN 61000-6-3 or any that subsequently apply at the time of manufacture.
- 1.4.8 The equipment (final assembly and sub-assemblies) shall carry the CE mark. Any subsequent final assembly of sub-assemblies shall carry the CE Mark and comply with the Construction Products Regulation 305/2011/EU or any that subsequently applies at the time of manufacture.
- 1.4.9 Lighting shall meet low light pollution requirements where defined in site specific Planning and Consent and be energy efficient.
- 1.4.10 Lighting shall comply with local planning constraints.

2 PERIMETER SECURITY

Strategic Intent

Provide a perimeter protection system that shall, demarcate National Grid secure perimeters for each site (which may or may not be concurrent with land ownership), deter, detect and delay unauthorised access to National Grid sites. (Forming an integral part of the physical ISS).

2.1 Functional Requirement

- 2.1.1 Demarcate the security perimeter for the site and appropriately secure the boundary of the site (fencing or physical barrier).
- 2.1.2 Provide a PID system to detect intruders attempting to gain access to the site.
- 2.1.3 The design and construction should deter attempts at climbing, breaching and burrowing beneath the fence / physical barrier and access / egress gates.
- 2.1.4 Where required by Operations the physical barrier system and gates shall be adaptable to be able to cope with temporary construction work on site. The integrity of the perimeter with regards to the functions described in this TSS should be maintained, taking into account any temporary fencing / security measures that may be installed.
- 2.1.5 A vehicle and pedestrian airlock shall be installed on substations which are visited on average, by at least one person, three days a week. The purpose of the airlock is to minimise the risk of 'tailgating' legitimate access either by vehicle or pedestrian.
- 2.1.6 In double fence lines, pedestrian and or maintenance access gates shall be incorporated for access to the sterile area between the two fence lines. These gates should be internal

operation only and secured by approved padlock. This can be located in the airlock where appropriate.

2.2 Equipment

2.2.1 The physical barrier will be a CPNI Protection Level BASE and National Grid previously approved security fence or wall as a minimum requirement.

2.2.2 The physical barrier shall be a minimum height of 2.4m, with an “electric” fence backing of 4.0m from the ground (extended at least 1.6m above the physical barrier) or 3.0m with MPID system and three strands of barbwire and /or video analytics, or MPID system with an “electric” fence topping of 1.6m.

2.2.3 The physical barrier shall surround the installation.

2.2.4 All perimeter barriers will incorporate an anti-burrow sill that is a minimum of 300 mm wide x 350 mm deep or as detailed in the ISS project GDM.

2.2.5 Where MPID is being installed, stock fences should be installed.

2.3 Perimeter Intrusion Detection System (PIDS)

2.3.1 The PID system shall integrate with the ISS access control, CCTV, and security lighting.

2.3.2 The PID system; which comprises of 1 or more of the following components EPID, MPID, Video Analytics, and Thermal Imaging, will be a CPNI and National Grid previously approved PID system and shall be stipulated in the SSOR.

2.3.3 The PID system manufacturer / installer shall supply a minimum of a certificate of conformity to National Grid and the Technology partner to confirm that the PID system installed has been designed, installed, commissioned as per the approved commissioning document and tested to the CPNI Protection Level as per the CPNI Catalogue of Security Equipment (CSE).

2.3.4 The PID system shall be configured to achieve a false alarm rate of no more than 7 false alarms per kilometre per day.

2.3.5 The PID system shall generate an alarm if an intrusion is attempted. For EPID systems this should occur whether the system is in HV or LV detection modes.

2.3.6 The PID system shall be zoned so as to work effectively in conjunction with the CCTV cameras within the zone. Gates shall each be separate zones to the adjacent fence zones. The PID system shall be able to support different configurations (e.g. EPID detection mode (LV) / HV modes) when the site is occupied or not occupied.

2.3.7 The EPID system should be capable of operating in (horizontal) split zone configuration. The number of zones is to be determined on a site by site basis with a maximum of two. These zones should be able to operate in different modes, when the site is occupied, typically with the lower zone(s) in detection mode (LV) and the upper zone above 2.4m in HV.

2.3.8 The PID system shall be capable of having all and individual zones disarmed when required.

2.3.9 The PID system shall be capable of being remotely controlled and monitored from the ARC.

2.3.10 On PID systems other than EPIDS, entry and exit shall be visually indicated (maximum of 30 seconds) via a vertical stack, 3 aspect (red, amber, green) traffic light system with integral hoods to prevent other light source interference and audible sounder. This shall be located inside the perimeter security fence in a location viewable by pedestrians and / or vehicles drivers as appropriate situated outside the gate or gates, indicating the following:

Red – PIDS on.

Amber – PIDS status not confirmed (e.g. communication's fault).

Green – PIDS on, VA not in sterile zone off (refer to 2.3.17).

2.3.11 On EPID systems, entry and exit and the associated operation of the electric pulse fence shall be visually indicated (maximum of 30 seconds) via a vertical stack, 3 aspect (red, amber, green) traffic light system with integral hoods to prevent other light source interference and audible sounder. This shall be located inside the perimeter security fence in

a location viewable by pedestrians and/or vehicles drivers as appropriate situated outside the gate or gates, indicating the following:

Red – PIDS / HV on.

Amber – PIDS status not confirmed (e.g. communication's fault).

Green – PIDS Detection mode (LV).

- 2.3.12 A fence check feature able to be used at any time that the site is manned should be incorporated into the EPID system, this should provide a visual indication of the fence status to Operations staff inside the site, without having to go to the site work station. The traffic light system above should be utilised with red indicating that the EPID system is in HV and green in detection mode (LV). This should be installed internal to site and in the vicinity of the above traffic light system.
- 2.3.13 Protection for culverts drains and cable trenches will be included in the perimeter security where they allow access in to site.
- 2.3.14 All perimeter gates including internal gates fitted with gate contacts shall be closed to allow the PID system to arm, with a facility to override this facility if required.
- 2.3.15 The EPID system shall be configured so that when the EPID system is armed and is operating in HV mode the LV FIM monitoring system is disabled to reduce alarms generated whilst in HV.
- 2.3.16 Where possible HV switches should not be deployed on the EPID system, alternative methods of physical isolation should be utilised. Refer to ISS project GDM.
- 2.3.17 When VA is installed monitoring a sterile zone, alarms shall be enabled when the site is occupied. When VA is installed, but not monitoring a sterile zone, these alarms should be disabled when the site is occupied.

2.4 Gates

- 2.4.1 Gates should incorporate a PID system, which is capable of:-
- detecting an attempted intrusion;
 - transmitting the alarm to an appropriate location (remote and local);
 - interacting with the ISS (for access control verification);
 - being configured to not alarm when the gate is accessed utilising the AACS.
- 2.4.2 When a gate is open for any circumstances CCTV cameras should automatically be triggered to focus on the entrance. Lighting should also be activated in levels of low ambient lighting/darkness to support CCTV and ARC operator visibility.
- 2.4.3 A local audible alarm shall indicate that the gate is open, after a predetermined time a remote alarm shall be activated. This alarm shall initiate immediately on emergency pedestrian gates, after 30 seconds on pedestrian gates and after 120 seconds on vehicle gates.
- 2.4.4 Gates shall be fitted with lock and bolt position monitoring to confirm that gates are fully closed and secure, these require separate alarm conditions.
- 2.4.5 The gate locking mechanism shall be capable of supporting a fully automated access control system.
- 2.4.6 Motorised gates, where fitted, shall be capable of powering gates up to 4m high, and the drive mechanisms for these gates shall be protected from physical interference.
- 2.4.7 Motorised gates where fitted shall have the facility to disengage for manual operation during power failure but still maintain their security function.
- 2.4.8 Motorised gate opening and closing times shall conform to 0.2 metres per second or up to 0.4 metres per second if fitted with a frequency converter.
- 2.4.9 Where Panic gates are required or currently exist they shall be incorporated as part of the physical security barrier to allow immediate egress from site whilst preventing access from

outside of the perimeter. These shall be designed to reset without affecting their primary function.

- 2.4.10 To fully meet National Grid requirements, panic gate internal centre plates and adjacent gate posts require being readily identifiable in the event of an emergency. To achieve this self-adhesive high visibility reflective tape product with a life expectancy of at least ten years, and suitable for application to all surface finishes should be applied to the internal gate centre plate and adjacent gate posts.
- 2.4.11 Panic gates shall be operated from inside the perimeter, fire regulations require a single action release mechanism, for example a 'crash bar or pad' (shielded so that it cannot be operated from external to the site).
- 2.4.12 Pedestrian gates shall be constructed to the same CPNI and National Grid approved classification as the physical perimeter barrier within which they are incorporated. One of these gates or both on a site with an airlock shall incorporate a mechanical lock to enable access to site in the event of a power failure. (See Section 3.3 Manual Access Procedure MAP).
- 2.4.13 Vehicle gates shall be constructed to the same CPNI and National Grid approved classification as the physical barrier within which they are incorporated.
- 2.4.14 Where a gate is hinged it shall be designed to resist removal.
- 2.4.15 Sliding gates shall be designed such that they cannot be removed by lifting or levering.
- 2.4.16 It shall not be possible to gain access under the gates, Refer to BS 1722.
- 2.4.17 It shall not be possible to externally bypass the security of the gate lock.
- 2.4.18 The gate design shall not incorporate potential footholds or other climbing aids.
- 2.4.19 All perimeter manually operated pedestrian gates (excluding Panic gates) shall have the facility to padlock them shut in the event of a lock / AACS failure, the padlock provided shall be a CPNI Protection level BASE padlock suited the same as the MAP vault lock. The emergency locking mechanism shall be fitted on the attackers' side, protected with a shroud and designed to prevent use as a climbing aid.
- 2.4.20 All perimeter manually operated twin leaf and powered perimeter vehicle gates shall have the facility to padlock them shut in the event of a lock / AACS failure, the padlock provided shall be a CPNI Protection level BASE padlock suited the same as the MAP vault lock. The emergency locking mechanism shall be fitted on the defenders side.
- 2.4.21 Where possible the Padlock provided above in 2.4.16 should be stored in the cabinet containing the manual override control equipment with signage / user instructions detailing operation.
- 2.4.22 Gates should be fitted with Surelock McGill / Pickersgill Kaye locks or other similar CPNI Protection Level or higher rated locks, previously agreed with National Grid.

2.5 Airlocks

- 2.5.1 The airlock system will be fully integrated with the access control system and the PID system.
- 2.5.2 The airlock shall operate with separate access requests for each gate. The airlock shall be configured such that all inner and outer gates shall be interlocked so as not to open at the same time. The airlock shall have the following local / remote functionality:
 - a) Remote ability to open the outer vehicle gate – complete one open/close cycle.
 - b) Remote ability to open the inner vehicle gate – complete one open/close cycle.
 - c) Remote ability to open the outer pedestrian gate – complete one open/close cycle.
 - d) Remote ability to open the inner pedestrian gate – complete one open/close cycle.
- 2.5.3 These remote operations shall be controlled by the Gate Monitoring Station (GMS) by a card and PIN action. Any readers/buttons will be clearly labelled. A screen displaying the associated airlock cameras and intercom camera will be fitted on site to aid with visitor

identification and to aid the operator in allowing safe ingress and egress of site, an intercom system shall be installed to allow two way communications with the gate intercom, with clear camera views of personnel entering, leaving, and moving through the airlock on their way into and out of site. The GMS does not require being located in a hardened room.

- 2.5.4 Vehicle Gate Interlock Override – Site shall have the facility to override the above interlock and open both gates together. The override will generate a 2 minute delay and an alarm at the ARC before opening the gates. This will reset to the previous operating model (normal or one gate open) when the activation process is followed a second time. This facility will be situated near the airlock and agreed by site. This function should not affect the site occupancy figures.
- 2.5.5 Vehicular and pedestrian access shall be demarcated in the airlock ensuring pedestrian safety at all times.
- 2.5.6 The inner and outer gate shall be spaced at a minimum of 10m apart with an optimum of 18m, with side fencing joining the two gates.
- 2.5.7 The airlock design shall incorporate an emergency pedestrian gate for egress from the airlock to the exterior of the secured site. A panic alarm button shall be incorporated within the airlock.

3 ID AND ACCESS CONTROL

Strategic Intent

To have a single access control system across National Grid UK businesses that provides an individual identification card with combined electronic access to sites and offices.

3.1 Functional Requirement

- 3.1.1 In the event of an AACS failure (including database failure) or loss of communication to the ARC, the local access control readers / system should continue to control and monitor access/egress onto/off site.
- 3.1.2 The AACS shall control access through nominated access control points at both commercial and operational sites.
- 3.1.3 The AACS shall be capable of defining and managing specified zones at a location where access is to be controlled. This will include designated access/egress routes and vulnerable areas and will support temporary changes to boundaries and zones.
- 3.1.4 Access control cards not presented to the card readers at the Site main entrance reader will not be able to operate other AACS readers on site.
- 3.1.5 The AACS shall be capable of interacting with other components of the ISS implemented at a location including PIDS, barriers, internal IDS, CCTV and security lighting systems that will provide additional confirmation of actual and or attempted access.
- 3.1.6 In emergency situations the AACS shall be able to release all controlled areas, lock down areas or restrict access.
- 3.1.7 All security doors and perimeter gates shall fail secure.
- 3.1.8 Security doors should be configured in one of three ways, both on entering or leaving a room or building. This will be as identified in the SSOR. The system shall allow the access control / locks fitted to doors to be switchable between “Normal Security” and “High Security” operating modes, this will be activated by the press of an icon on the ARC workstation or locally on the site ISS AMS Server. Each door will have an IN Normal, IN High, OUT Normal and OUT High identified in the SSOR. The associated door alarms will need to be configured accordingly. The free access configuration is not required to be supported by the backup/ UPS power supply. The three ways are :-
 - a) Free Access
 - b) Access control card
 - c) Access control card and PIN

3.1.9 The card reader system should be capable of working with different types of card technologies as specified on a site by site basis.

3.1.10 The authorisation of individuals' access permissions shall be capable of being devolved to the accountable site owner (occupier) and manager via the on-site ISS AMS Server.

3.1.11 All locks shall be 100% duty cycle rated solenoids to allow free access.

3.2 Equipment

3.2.1 The access control system shall function utilising a single individual ID Access Security Card across all sites employing an associated integrated security control system.

3.2.2 The access control system shall be capable of granting an individual access on the system with the appropriate permissions; the system shall also have the ability to manage against individual skills and competencies (override by explicit authorisation only).

3.2.3 The AACS shall be capable of providing occupancy counts.

3.2.4 The AACS shall be able to generate an alarm if a door is left insecure, forced or when an invalid card is presented to the reader.

3.2.5 The mode of access control shall be:

- a) Proximity cards
- b) Proximity cards plus PIN

3.2.6 The AACS cards shall as a minimum meet the following requirements:

- a) HID iClass Proximity card
- b) 13.56 MHz contactless Smart card
- c) 125 kHz HID Proximity card
- d) 16k configurable memory
- e) Facility Code 30

3.2.7 Where the contractor is required to supply the AACS cards, agreement will be required by National Grid prior to the configuration of the AACS as to the compatibility of the cards.

3.2.8 Access Cards shall be physically capable of working in high voltage substation Etx environments, being intrinsically safe, withstanding high voltage EMF's and meeting National Grid's requirements.

3.2.9 Card readers that are external to the site shall be configured to require card plus pin access and be fitted in vandal resistant housing. Other readers may also require PIN numbers on a site specific basis.

3.2.10 Access control shall not be fitted in environments deemed to require intrinsically safe equipment. This will require approved manual locking.

3.2.11 The AACS shall be able to restrict certain levels of access. The AACS shall be able to manage changes to access permissions and inhibit specific door alarms at short notice, or in advance, with the ability to cancel any card immediately.

3.2.12 The existing site intercom or site visitor phone shall be remaining or be reinstated where required. This shall be covered with CCTV to allow recognition which shall be displayed on the GMS. Refer to the CCTV section.

3.2.13 Disabled access requirements should be considered in line with building regulations and for all new build sites, in line with SSR guidance.

3.2.14 AACS with card only should be fitted internal to the vehicle and pedestrian gates for card presentation to exit site.

3.2.15 All external card readers shall have tamper alarms enabled.

3.3 Manual Access Procedure (MAP)

3.3.1 The purpose of the single site suited Manual Access Key is to provide access through the main pedestrian gate(s) and to the rooms that hold the ISS AMS server and rack, UPS power supply and the access controlled key safe (where fitted)

3.3.2 The site suited Manual Access Key and access controlled key safe key should be stored in the CPNI approved Manual Access vault unless otherwise specified. The exact location shall be agreed with Site operations and the ISS team.

3.3.3 The alarm outputs, inputs and video images should be integrated into the ISS.

3.4 Operation

3.4.1 The access control system shall interface with site plans and interactive icons representing the location and real-time status of access control and alarm monitoring equipment.

3.4.2 The AACS shall be able to enforce anti-pass back controls.

3.4.3 The AACS shall be configured in such a way that where sites are of shared occupancy, the system is capable of being configured for authorised access to the 3rd party.

3.4.4 The AACS shall be capable of providing duress alarms.

3.4.5 Access to designated sites shall be controlled via the AACS. This includes any access / egress points except egress via emergency exits, entrance to site perimeters via main gates, entrance to buildings within operational sites and specified zones.

3.4.6 The AACS shall be configured to allow manual override of gates and access on site remotely by the ARC.

3.4.7 The AACS shall enable the electric fence (where fitted) to automatically activate into HV mode when the last person leaves site.

3.4.8 The AACS shall be able to isolate local detection zones when vehicle and pedestrian gates are in use and for 20 seconds after their closure. The intent is to reduce the risk of false alarms when combined with MPID and/or VA systems covering the access area. The duration of the above time delay shall be configurable by the ARC as an engineering function.

3.4.9 The AACS shall be capable of providing and managing authorised access groups (as well as being able to assign access to authorised individuals) enabling import and download as well as different security levels, enabling a change within a 'ping round trip' duration (typically less than 1 second) in security status to be reflected in the management of sites.

3.4.10 Where applicable, contractors' access rights should be restricted to the areas required to fulfil an individual's job role.

3.4.11 The AACS shall provide a complete management (audit) trail.

3.4.12 The system should activate security/safety lighting on personnel entering and leaving site and light the route to and from the Control building where it exists during hours of darkness, when staff are on site.

3.4.13 The AACS shall be capable of releasing all doors on exit routes. Unless otherwise stated, security doors and perimeter gates will fail secure, but be fitted with Request to Exit (RTE) Button, push bar / pad or thumb turn emergency exits and key override (to be kept in the access controlled key safe) for ingress.

4 CCTV

Strategic Intent

The principal purpose of the CCTV system is to verify site intrusion following a perimeter alarm so as to allow an immediate police response to be requested. The secondary purpose is to provide a search facility, after an alarm, to attempt to provide further information to the police regarding the intruders.

In addition the CCTV system will be capable of producing high quality video evidence suitable for use after an event, e.g. in support of a prosecution. Please see also CAST CCTV Guidance documents.