RISCAuthority

administered by

FPA Fire Protection Association

S33 Solar farm security

Version 1 Published 2020

Cover image: iStockPhoto/killerbayer

Acknowledgement: The assistance of The Lyndhurst Consultancy in the preparation of this guide is gratefully acknowledged.

Contents

1 A security challenge

The theft of PV panels and, especially, cabling from solar farms, has emerged as a serious problem for operators and insurers. The security challenge is unique. A typical solar farm consists of a concentration of significant value placed in a totally rural situation which may enjoy little or no natural surveillance from residents or passers-by.

2 Targeted assets

Both cabling and panels are exposed to theft but it is the potential value of the cabling as scrap that seems of most interest to criminals. Experience to date would indicate that 6mm inverter cables are of the most interest. These are usually exposed under the panel arrays and are easily removed, particularly where they are grouped together at the end of an array, being bunched together in long lengths making it very easy to remove large quantities at a time. Larger AC and HV cables tend to be buried underground and seem less exposed to theft as a result.

Alamy/PhotoPower

Figure 2: The inverter cables cut at each end by thieves for removal

iStockPhoto/LL28

Figure 1: Inverter cables running sometimes over 100m along a conduit under the array

3 Security planning

Needless to say, securing the site of a solar farm is very expensive. To help minimise the need for costly piecemeal measures required to remedy security weaknesses that become apparent during the life of the operation, management should collaborate with interested parties such as insurers, brokers and security providers at the initial planning stage and prior to any enlargement of the facility. This will allow security budgets to be accurately costed at the outset and the chance of poor spending decisions will be minimised. Choice of a location well away from public rights of way and other access points is a critical factor.

Reliable detection of unauthorised persons on site is absolutely essential and all options for selection of the most effective technology must be considered against an assessment of the penetration risk for the site in question. Even then security will be critically impaired from the start if there is no effective physical barrier around the perimeter (eg a security fence) to impede intruders who might otherwise freely approach the security equipment within the site with a view to disabling it.

4 The perimeter

Alamy/Ingemar Magnusson

Figure 3: Interlocking concrete blocks but each may need to weigh up to 4.5 tonnes

4.1 Security fencing

The entire perimeter should be secured to a consistent standard by security fencing. A fence consisting of so-called '358' welded mesh panels to BS 1722-14 *Fences: Specification for open mesh steel panel fences* is ideal. It should reach 3m in height including a canted-out topping of barbed wire or razor tape. An ample number of signs should be attached to the fence warning of the dangers of attempts to climb it. To frustrate burrowing under the fence line the mesh can be extended below ground level. All openings must be gated to the same standard and gates are recommended to be secured by welded-on high security locking bars and equivalent padlocks. Ensure entry points are minimised, controlled and monitored, locally or remotely, so that only authorised personnel are allowed access. Guidance on gates and locking devices is to be found in various parts of British Standard BS 1722-10.

4.2 Hostile vehicle attack

Typically, intruders aim to get a vehicle on site and, working at night, they will feel they can apply extreme force with confidence, possibly using a vehicle to force entry. Consequently the specification above should be seen as a minimum standard and radical action may have to be taken to prevent penetration with a vehicle. Security providers accustomed to protecting against ram raid, ie hostile vehicle mitigation (HVM) measures, can be approached to propose physical measures for openings capable of providing HVM protection that is significantly superior to normal locking methods. Earth embankments around the site will protect against use of a vehicle against the fence itself. Alternatively, interlocking concrete blocks weighing up to 4.5 tonnes can be placed across any sections of the perimeter remaining vulnerable to vehicle attack.

5 General site security

5.1 Video surveillance

A skillfully designed video surveillance (CCTV)system is essential. In the case of a solar farm a detector activated system will be required signalling to a police recognised remote video response centre (RVRC) and conforming to BS 8418. The installer must be approved by one or other of the police recognized Inspectorate bodies, the NSI or the SSAIB, provide a maintenance contract and secure a police unique reference number (URN). The system design should ensure that thieves in the act of removing PV panels, cabling and the equipment housing inverters, anywhere on site, stand a high probability of being detected. It should also extend to include opening contacts fitted to site gates. The most effective system design would, in addition to the CCTV coverage of the PV panels and supporting components, ring the site inside the perimeter fence with static cameras having overlapping fields of view that follow the fence line, allowing a high probability that intruders who have successfully penetrated the fence will be detected almost immediately as being on site.

The audio challenge facility of the system should be activated and play a suitable announcement if an alarm occurs. Automatic number plate recognition (ANPR) should be included to capture and record the registration mark of vehicles entering the site. The integrity of the connection to the RVRC should be monitored by an alarm transmission system conforming to grade DP3 of BS EN 50136-1.

6 Additional remarks

6.1 Choice of detector

A detector activated CCTV system usually consists of cameras in association with external passive infrared (PIR) detectors which, when triggered by an intruder, cause the associated CCTV camera to send images to the RVRC. However, given the dimensions of a large solar farm it might be determined that strategically located active beams in pre-built towers, or microwave fence detection systems, are likely to give better results as triggering devices than the normally employed PIR technology.

iStockPhoto/wbritten

Figure 4: Perimeter alarm protected site

6.2 Video analytics

In the situation of a fenced solar farm (ie a so-called 'sterile zone') the technology known as Video Analytics (VA), sometimes referred to as Video Content Analysis (VCA), offers potentially superior discrimination between intruders and other sources of disturbance. The image analysis is performed by software residing in the system equipment which examines the image captured by the camera. This obviates the need for separate traditional detectors. VA performs better in this type of situation than any other. Although it has attracted interest as having near-human powers of image analysis against terrorists, urban criminals etc, its main benefit is containment of the false alarm rate of external systems. The technology can differentiate between active human beings on site and sources of false alarm such as blowing debris or activities outside the perimeter that might trigger a conventional detector. The services performed by the RVRC are the same for systems triggered by VA as those triggered by discrete detectors.

6.3 Operation in darkness

The site is unlikely to have artificial lighting sufficient for a standard CCTV system or any at all. Consequently, infrared (IR) lighting will need to be provided. In this situation, long-range narrow beam LED IR luminaires will be needed. Alternatively, the CCTV provider may propose a system comprising thermal imaging cameras. In a detector-activated type system the control equipment generates an alarm signal for the RVRC generated by the IR radiation emitted by a moving intruder. Increasingly, so-called 'edge detection' techniques allow the software to be integral to the camera itself, simplifying installation and commissioning. Thermal imaging cameras give satisfactory results irrespective of lighting levels and this technology is increasing in popularity as there are benefits over the conventional image capture technology of the standard camera. There is, however, a cost penalty.

7 Other site security solutions

Although the provision of state-of-the-art video surveillance must be seen as the primary defence, there is a range of additional site security solutions from which to choose if supplementary security is necessary or otherwise desired.

7.1 Perimeter intrusion detection (PID)

Proprietary fence detection systems such as continuous microphonic cable is capable of giving excellent results as it will trigger camera(s) as soon as interference with the fence is detected (but see 'false alarm control' below). Inside the fenced zone itself, buried security devices are available to detect human beings moving on site. Miniature geophones detect seismic disturbance, fluid-filled rubber tubing is designed to detect movements on a pressure-differential basis whilst another product creates an alarm if an intruder disturbs an electric field created by buried cables. These solutions have been developed over time and can give acceptable results, depending on the terrain and ground conditions but there are trenching costs of course and the susceptibility to false alarms of the particular technology needs careful examination in advance.

7.2 Manned guarding

At times of heightened vulnerability, especially following a successful raid and, perhaps, pending the implementation of strengthened security solutions, management may have no alternative, if escalation in criminal activity is to be avoided, but to retain an on-site guarding service until renewed confidence can be had in the technical security measures. Only those firms conforming to BS 7499 Static site guarding and mobile patrol service – Code of practice, and registered by the Security Systems and Alarms Inspection Board (SSAIB) or the National Security Inspectorate (NSI), should be considered. Failing that, the selected firm should at least have the approval of the Security Industry Authority (SIA) Approved Contractor's Scheme (ACS). There should preferably be at least two guards in attendance when the site is unoccupied or sparsely attended. The guards should be in continuous radio contact with each other whilst patrols are conducted, preferably monitored for audit purposes, by an electronic 'clocking system'.

7.3 Security management

iStockPhoto/seroz4

Figure 5: Security fences can be enhanced by variou means

The perimeter should be regularly inspected and the details logged. A criminal technique is to degrade the security at a given point over a period of time in advance of a carefully planned raid. Signs of criminal activity seen on an inspection should be acted on by enhancing surveillance and informing the police.

Clear instructions should be agreed in a response plan or service agreement outlining the actions required after any alarm activation or fault signal. These must include contact and liaison with the response authority (normally the police), keyholder attendance and emergency corrective maintenance. Keyholders, whether employed by the site operator, or a commercial keyholding service, should undertake to attend site within 20 minutes of being notified that a request for police attendance has been made. This is required by the police in their Security Systems Policy. Other notifications from the RVRC that have not given rise to a request for police attendance, eg hostile or suspicious activities on the part of third parties or a fault with a critical part of the installation, should be responded to by keyholders within 30 minutes to one hour.

No permanent changes to the security system, its configuration or a greed performance should be made without reaching agreement with the insurer.

7.4 False alarm control

Wildlife cannot be eliminated completely but it must be minimised, otherwise electronic video surveillance will not be practicable. If, for whatever reason, the site has not been protected with security fencing as recommended above, the entire perimeter, including gates, will still need steel mesh wildlife exclusion fencing to a height commensurate with the wildlife in the

Figure 6

area eg if deer are present, the fence may need to be 1.8/2m high. If burrowing animals are present, the bottom edge of the mesh should be turned outwards and buried a minimum of 150mm. Where the site does have a perimeter security fence which has a penetration system attached to it, an additional outer wildlife fence may be unavoidable to control excessive false alarms with the penalty of additional cost.

7.5 Enhanced security for PV panels and cable

Security targeted specifically on the panels and cable connections should be considered only as supplementary to the site security measures outlined above which should be seen as the priority.

Measures to protect PV panels

A variety of proprietary panel fixing devices is available designed to frustrate the ready removal of panels using everyday tools, 'tighten-and-break' screws being an example. Such devices should force thieves to resort to powertools which buys time during which their detection/ apprehension is more assured. Electronic detection products are also available capable of detecting panel removal and it should be possible to include these in the automatic detection system for the site itself.

Measures to protect cable

Cable buried in trenches and then clamped in position buys valuable time. Proprietary anti-theft clamps are available. Electronic devices are also available that create an alarm signal should lengths of cable be interfered with or disconnected.

Forensic cable marking products such as Smart water [https://www.smartwater.com/] are widely employed and recognised by criminals and the scrap metal trade. Warning notices are supplied with these products which should have a deterrent effect with certain thieves.

8 More information

For more information see RISCAuthority guides:

- *Site security: external alarm protection*
- *Site security: fences, walls and gates*

These may be downloaded from www.riscauthority.co.uk

RISCAuthority

administered by FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk