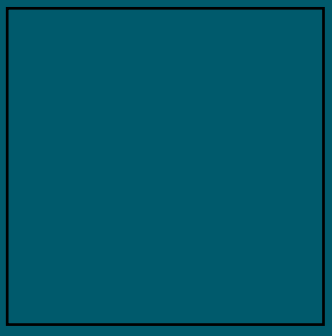
Loss Prevention Standards – Asset Classes

Ground Mounted Photovoltaic Solar Farms Security

Version: 1.2
Date: 24th October 2024



Ground mounted, grid scale, PV/Solar farms are becoming increasingly common. Whilst acknowledged as a sustainable means of generating energy, the construction, operation, and maintenance of PV/Solar systems presents a number of hazards requiring careful consideration and management. This document is one of a series, providing guidance to help identify and mitigate the risks related to ground mounted PV/Solar Farms.

AVIVA

Ground Mounted Photovoltaic Solar Farms Security

Introduction

Ground mounted Photovoltaic (PV)/Solar Farms are typically located in remote, rural areas. Security measures are often limited, and they are also mainly unmanned with personnel only attending site for repairs, maintenance, inspections as required etc.

These factors combined with the resale value of PV/Solar panels, cabling, metal, and other components, means PV/Solar Farms are often targeted by thieves. which can result in significant damage to infrastructure, expensive repairs, and loss of revenue whilst the system is impaired.

In terms of statistics, Police in the UK observed a 93% rise in reports of solar-related crimes from 2021 to 2022. That figure included a rise in small-scale thefts of solar panels. In August 2023 thieves removed 80 PV panels, valued in the region of £10,000 from a PV/Solar Farm in Wellingborough, damaging infrastructure and site security protections. Based on Aviva claims detail, four PV/Solar Farm theft incidents over a six-week period between December 2023 and February 2024 totalled nearly £250,000.

As well as physical theft, cyber security is increasingly prevalent. Aviva research carried out in 2023 across UK companies found 20% admitted suffering a cyber-attack or online fraud in the past year. The research found that businesses are 67% more likely to have experienced a cyber incident than a physical theft, and almost five times as likely to have experienced a cyber-attack as a fire. A cyber-attack on a solar farm in Japan intended to access financial information, was discovered in June 2023 when malicious actors hijacked 800 SolarView Compact remote monitoring devices.

Implementing appropriate security protections can significantly reduce the risk of incidents, such as those highlighted above, and help reduce the extent of theft damage.

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Overview of common security risks

Theft

PV/Solar Farms can be targeted by both opportunistic thieves and organised criminal gangs. Ease of access to sites, and the often-limited security measures in place means sophisticated equipment and planning is not necessary to carry out a successful theft attack.

Theft attractive equipment includes the copper 'string cables' attached to the rear of the panels and/or supporting frames, which are targeted for their high scrap value. It is also relatively easy to isolate sections of string cabling, making it simple and safer to remove. Large sections of buried copper transmission cables are extremely attractive to thieves, and whilst not as simple to remove as string cabling, can be pulled from the ground with little force and basic equipment such as All-Terrain Vehicles (ATV's), vans and trucks.

PV/Solar panels themselves are also vulnerable and are considerably easier to remove than sections of heavy cabling. The panels contain significant amounts of copper which can be recycled and sold as scrap, however increasing energy costs has resulted in panels and components being stolen and resold for energy generation purposes.

Given the size and weight of PV/Solar equipment, vehicular access is generally needed however, sites are often secured by lightweight fencing, gates, chains, and padlocks, designed for livestock containment rather than security

protection, and which are easily bypassed. PV/Solar Farms will generally feature vehicular access routes between arrays for maintenance and inspection purposes, meaning vehicles can move around sites with little difficulty.

Vandalism

Whilst not as common as theft, vandalism can cause significant damage and disruption to ground mounted PV/Solar systems, particularly monitoring equipment and the inverters, transformers and substation which are critical components to the site's export capability.

Security Vulnerabilities

There are certain features that can make ground mounted PV/Solar Farms more vulnerable to attack by thieves or vandals:

- Proximity of escape routes - Thieves target sites with good access to main roads for escape purposes.
- Site theft history - Sites with a history of theft are also more likely to be targeted again, as the vulnerabilities are known to the thieves. 61% of victims of solar energy crime are repeat victims, with either themselves or a site within 5 miles being targeted.
- Local exposures – Thefts or rural/countryside crime in the locality may suggest thieves or criminal gangs are operating in the area, which increases the potential for theft at the site. Proximity to schools, towns and large villages may present an increased vandalism risk, particularly during holiday periods.
- Security protections - Sites with weak security measures are vulnerable to theft incidents. Concerns include:
    - Perimeter security - Insufficient or lightweight perimeter fencing facilitates ease of access to sites by foot or vehicle.
    - Detection security – Good quality detection security such as Visual Surveillance Systems (VSS), movement alarms etc., provide a strong deterrent to thieves, whereas a lack of, or sub-standard detection arrangements and insufficient monitoring means persons accessing the site will have increased, or in some cases unlimited time to effect damage. VSS recordings may also aid identification of intruders and support criminal proceedings.
    - Lightweight padlocks and chains – Lightweight padlocks and chains can be easily forced to gain access to the site.
    - Key boxes – Lightweight key boxes located outside the site, used to hold access keys to buildings and locks can be easily forced and the site accessed.
    - Security lighting - Poor lighting allows thieves to operate undetected.
- Security Management – Lack of security planning, inspections, and an unfocussed security management approach can leave the site vulnerable to theft attack.
- Cyber Security – With the PV/Solar system and some security protections being monitored, cyber-attacks can compromise security to enable data theft, install ransomware etc.

Security Management Plan

An effective security management plan comprises several individual security measures that combine to provide a 'layered' level of security protection, designed to deter, or at least hinder unauthorised access to the site, provide

suitable warning of any theft attack or unauthorised access, and detail the sites response planning to such incidents.

Risk Assessment

Undertaking a Security Risk Assessment helps identify:

- Gaps or omissions in the site management such as ownership, co-ordination, and communication issues etc.
- The vulnerable assets at the site.
- the likelihood of a theft incident occurring based on local knowledge, local crime data, sector trends including local police response to incidents.
- The likely extent of any intruder related damage.
- The impacts to energy production and site profitability.
- The adequacy of current security arrangements.
- Necessary improvements to the security arrangements.
- Gaps in security knowledge and potential supplier competencies.
- Security review arrangements.
- Cyber security measures.

The risk assessment should be undertaken and reviewed by persons with a working knowledge of the site and its vulnerabilities, good knowledge of the locality and any recent local theft or malicious activity, experience in providing security protection in rural, outdoor, unmanned sites and someone able to make or influence security funding decisions. The use of a Security Consultant, preferably one registered with the Register of Chartered Security Professionals, and with a speciality in PV/Solar Farms and rural crime should be considered.

The risk assessment should be recorded and routinely reviewed, particularly at the initial planning stages of the site, upon completion and/or upon unauthorised access or attempted access being made at the site. This will allow for appropriate security measures to be installed at the appropriate time and help with next phase security measures. Responsibility for oversight of any control measures identified in the risk assessment should be delegated to a responsible person.

It is advisable to discuss any planned security protections with your Insurer and Broker.

Perimeter Security

Perimeter security is the first line of defence and is also a deterrent to potential intruders. Three metre proprietary security fencing certificated to LPS 1175: Issue 8.1 Requirements and Testing Procedures for the LPCB Certification and Listing of Intruder Resistant Building Components, Strongpoints, Security Enclosures and Free-Standing Barriers and achieving a security rating of at least B3 should be considered for PV/Solar Farms or localities that have had issues with unauthorised access and/or theft or vandalism incidents, particularly to areas of the site perimeter that are accessible/approachable from public highways or footpaths.

Fencing types not achieving certification to LPS1175, whilst not providing a defined security resistance, may be suitable for lower risk sites, or areas of the perimeter that are not easily accessible. Such fencing, which includes 'V-Mesh' fencing types should be installed to a height of at least 2.5 metres and preferably in compliance with BS1722 Part 14: Fences Specification for Open Mesh Steel Panel Fences.

Whilst reliable detection of unauthorised persons on site is essential, site security will be compromised if there is no effective barrier around the perimeter. The use of lightweight 'chain link' style fencing, also known as stock or deer fencing is commonly used for PV/Solar Farm perimeter fencing however, provides negligible security protection and

should only be considered in areas where the site adjoins or borders private land with no common access to persons or vehicles, and where supported in the Security Risk Assessment.

The use of security ditches or terraforming can also help prevent or limit vehicular access to vulnerable perimeter areas, whilst the presence of dense and thorny shrubs or bushes can provide a deterrent to unauthorised pedestrian access. This should be considered within the initial security design stages to ensure planning applications adequately detail proposals.

Movement activated security lighting can also act as a useful deterrent.

Some wildlife, including burrowing animals, can damage security fencing and provide access opportunities to the site. This should be considered when designing fencing systems to ensure appropriate resilience.

Site Access

All entrance gates and gate posts should be of similar construction to the security fencing and be secured with good quality padlocks and heavy-duty chains. Padlocks should be in compliance with BS EN 12320:2012 Building hardware. Padlocks and padlock fittings. Requirements and test methods and achieve a CEN grade 4 or 5 rating. If possible, a steel protective lock housing of at least 4mm thickness should be fabricated to access gates to help prevent lock tampering. Keys for entrance gate padlocks should not be kept on site and any padlock combination codes changed regularly, particularly after key staff leave site. Digital combination type key safes are vulnerable to attack and are not recommended.

Gates hinges should be capped, or spot welded to help prevent ease of removal.

To protect site entrance gates from vehicular attack, particularly on sites that have previously suffered, or are deemed vulnerable to such incidents, the use of retractable or removeable security posts, preferably achieving Sold Secure Gold approval, should be considered. Alternatively, the use of large moveable objects such as traffic management boulders to block entrance routes may be beneficial, however any lifting equipment used to transport such objects will need to be effectively secured and if necessary isolated to prevent illicit usage.

Video Surveillance Security Systems

The most effective detection security for remote and unmanned premises is a detector activated Video Surveillance System (VSS) monitored by an accredited Remote Video Response Centre (RVRC) and achieving level 1 police response. The VSS should be positioned to cover all points of the site perimeter, site entrances, the PV/Solar arrays and the key equipment and buildings.

To achieve level 1 police response, the system will need to be installed, maintained, and monitored to the requirements of BS8418: Design, Installation, Commissioning and Maintenance of Detection-Activated Video Surveillance Systems (VSS). Code of Practice.

To ensure the best quality of service, the Installer and RVRC should be members of a UKAS third-party accreditation/approval scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB). This is required for any VSS requiring a police response.

To further improve the deterrent value of the VSS, the incorporation of an audio challenge facility, which would allow the RVRC to issue warnings to any unauthorised persons attempting to access the site or behaving suspiciously, should be considered. In areas with high crime rates or sites that have suffered previous or recent security concerns or incidents, the VSS can be extended to include Automatic Number Plate Recognition (ANPR) equipment to capture and record the registration mark of vehicles entering the site.

Mobile video surveillance systems with thermal imaging capability can also be added as a temporary measure following a site theft incident to temporarily enhance site security. Aviva claims data suggests a repeat theft attack, soon after the initial incident is very likely, and immediate security enhancements can help reduce this risk.

Cyber security exposures should be reviewed to ensure appropriate protections and procedures are incorporated including data access approval management.

The presence of wildlife at the site can lead to false activation issues, and potentially compromise police response to VSS activations. This should be considered in the system design and camera equipment that can differentiate between animals and potential intruders utilised where possible.

Specifications for your proposed detection security system should be submitted to your Insurer for review.

Security Company Response

Given the remote nature of many PV/Solar Farms, and anticipated delays in police response in some localities, it may be more appropriate to utilise a security company to provide keyholder and VSS detection response services, rather than rely on police response. Regular security patrols of the site by the security company can also provide a significant deterrent to intruders.

Any such providers should be members of the Security Industry Authority and provide their services in accordance with the requirements of BS 7984-3:2020 Keyholding and Response Services - Provision of Mobile Security Services. Code of Practice. They should also be members of a UKAS third-party accreditation scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB).

The presence of security signage in prominent locations such as entrance gates, perimeter fencing and near critical equipment and buildings can be a significant deterrent to intruders. Emergency contact numbers should also be provided for persons wishing to report any security concerns. Such signage should be installed at distances not exceeding 50 metres.

Staff keyholding and site response to VSS detection alerts is not recommended, unless in accompaniment of approved security guarding or the police.

Other Security

Site buildings should be adequately secured depending on the type of contents, attractiveness to thieves or potential for malicious damage. Lower risk buildings should feature good quality doors and door locks preferably confirming to British Standard BS 3621: Lock Assemblies Operated by Key from Both the Inside and Outside of the Door. Opening windows should be secured by key-operated window locks and the keys removed from the windows and secured appropriately.

External compounds, used to house any transformer and/or generator equipment etc., should be of robust palisade or 'V-Mesh' type fencing to a height of at least 2.5 metres and secured with good quality padlocks. A steel protective lock housing of at least 4mm thickness should be fabricated to compound gates to help prevent lock tampering.

Spare panels, cabling, valuable metal components etc., should not be stored in large quantities at the site, particularly during the construction process, and instead delivered to the site 'as needed' to prevent accumulations of theft attractive equipment.

All outdoor equipment cabinets for inverters, combiner boxes etc., should be securely locked, and any switch/control panels also secured to prevent malicious interference.

Security guarding should be considered during the initial site construction phases, should high volume of theft attractive components be held the site prior to installation, or in the event of continued security incidents or concerns.

Any such guarding company and staff should be members of and/or affiliated to the Security Industry Authority, should provide their services in accordance with BS 7499:2020 Provision of Static Guarding Security Services. Code of Practice, and be members of a UKAS third-party accreditation scheme, such as those provided by the National Security Inspectorate (NSI), or the Security Systems and Alarms Inspection Board (SSAIB).

The use of patrol dogs as part of your guarding or site response arrangements is recommended, however dogs should not be left alone to protect a property. This is expressly prohibited under The Guard Dogs Act 1975, with minor exceptions. The Animals Act 1971 also imposes duties which may result in the owner or keeper of the dog(s) being held liable for injuries and damage where a guard dog is responsible. There are exceptions, including deliberately ignoring warning signs, however advice should be sought from legal representatives and/or an accredited guarding company with guard/patrol dog handling experience.

The installation of a Perimeter Intrusion Detection system, which provides advanced warning of an intruder or threat approaching or attempting to breach site perimeter fencing should be considered, particularly where there have been recent security concerns in the locality. The sensors can be ground, or fencing panel mounted and detect vibrations as well as identify the locations under threat. Such systems are particularly beneficial when installed in conjunction with a VSS incorporating an audio challenge facility. Your electronic security company can provide more information.

Self-Inspections

Regular recorded inspections of the perimeter and security protections should be undertaken to check for signs of tampering, damage, cut fencing sections, animal related damage or issues, or unauthorised access. Such inspections should extend to fencing, fencing posts, gates, gate hinges, padlocks, VSS equipment, security signage etc. Any damage or faults should be repaired/reinstated promptly and investigated to gauge whether additional security protections or measures are necessary. These inspections should be completed at least monthly, or more frequently if there have been recent security concerns in the locality.

Emergency Response Planning

It is important to establish an appropriate Emergency Response Plan, to identify responsibilities and a planned set of actions to respond to security incidents including cyber security related incidents. These plans should be reviewed and updated regularly and owned by the site management, particularly following a security related incident, to ensure any remedial actions are completed.

Protection of Key Assets

Forensic or DNA marking is the application of a discreet agent, with a unique forensic signature, to mark valuable and/or easily removable items. Such marking can be applied to cabling including buried and string cables, PV/Solar Panels, and other valuable equipment onsite. Therefore, any recovered stolen equipment can be returned. Pairing with appropriate warning signage can also act as a valuable deterrent to thieves.

Any such protection should be applied by a competent and experienced company, and preferably members of the British Security Industry Associations (BSIA) Asset and Property Marking Section.

Spare panels and other theft attractive components should not be stored on site. If this is unavoidable, storage should be limited to essential spares only and kept within a secured and robust building. The physical security recommendations pertaining to higher risk buildings above should be followed. The use of shipping containers for storage of theft attractive spares is not recommended.

Backfilling underground cable runs or ducts with cement can reduce the risks of cable theft. A depth of at least 300mm is recommended.

Diesel for back-up generators should be limited to essential supplies only and secured within a secured building or security compound.

Key Action Steps

- Complete a Security Risk Assessment. A registered Security Consultant can assist with this.
- Identify the required security protections based on sector specific and locality issues.
- Discuss security plans with your Insurer and Broker.
- Use accredited companies and products.
- Implement a formal security inspection regime.
- Devise an emergency response plan.
- Routinely review security protections and plans, particularly following a security incident or local issues.

Checklist

A generic Security Checklist is available, which can be tailored to organisation's needs.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners, including:

- VSS and detection security: Secom.
- Forensic/DNA marking: Selectamark.

For more information please visit:

https://www.aviva.co.uk/risksolutions/specialistpartners/

Sources and Useful Links

- LPS 1175: Issue 8.1 Requirements and Testing Procedures for the LPCB Certification and Listing of Intruder Resistant Building Components, Strongpoints, Security Enclosures and Free-Standing Barriers.
- BS1722 Part 14: Fences Specification for Open Mesh Steel Panel Fences.
- BS EN 12320:2012 Building hardware. Padlocks and padlock fittings. Requirements and test methods
- BS8418: Design, Installation, Commissioning and Maintenance of Detection-Activated Video Surveillance Systems (VSS). Code of Practice.
- BS 7984-3:2020Keyholding and Response Services - Provision of Mobile Security Services. Code of Practice.
- BS 3621: Lock Assemblies Operated by Key from Both the Inside and Outside of the Door.
- LPS 1197: Issue 4.2 Requirements for the LPCB Approval and Listing of Companies Inspecting, Repairing and Maintaining Fire and Security Doors, Door sets, Shutters and Active Smoke/Fire Barriers.
- BS 7499:2020 Provision of Static Guarding Security Services. Code of Practice.

- The National Security Inspectorate (NSI).
- The Security Systems and Alarms Inspection Board (SSAIB).
- The British Security Industry Associations (BSIA) Asset and Property Marking Section.
- Security Industry Authority.
- The Guard Dogs Act 1975.
- The Animals Act 1971.
- Sold Secure.
- Register of Chartered Security Professionals.
- Fire Protection Association S33 Solar Farm Security.
- RiscAuthority Guidance Document S35 Internet of Things – Connected Security Devices and Systems.

Additional Information

Related Loss Prevention Standards include:

Aviva Risk Management Solutions LPS: An Introduction to Closed Circuit Television (CCTV) Systems
Aviva Risk Management Solutions LPS: Locks
Cyber Security: Top 12 Tips to Protect Against Cyber Attacks.
Cyber Security: The Internet of Things.
Cyber Security: Respond and Recover.
Cyber Security: Ransomware.
Cyber Security: Cyber Essentials Accreditation.

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666. *

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

24th October 2024

Version 1.2

ARMSGI732024