Onshore Wind Turbines – Security

Wind farms and turbines can be vulnerable to security related losses, with targeted cable theft being one of the main causes of such losses.

This Loss Prevention Standard discusses security protections and mitigations to help reduce the potential for wind turbine related theft damage.

Version: 1.1
Date: 26th August 2025

Onshore Wind Turbines - Security

Introduction

Wind turbines are more vulnerable than many other infrastructure types to theft attack. They are typically located in remote and/or rural areas, and security measures are often limited. They are also generally unmanned with workers only attending the site for repairs, maintenance and inspections when necessary.

These factors combined with the theft attractiveness of high-value metal cabling has resulted in a number of targeted attacks in recent times, including a number of turbine cable thefts in England from April to June 2025 and this cable theft incident in Scotland in July 2025. In addition to the physical damage to infrastructure and expensive repairs, the loss of revenue whilst the system is impaired can be very significant.

Whilst a site's security risk exposure may be perceived as low at the time of construction, the potential for criminal damage may increase over its lifespan. Implementing appropriate security protections can significantly reduce the risk of incidents, such as those highlighted above, and help reduce the risks of malicious and theft related damage.

Understanding the Risks

The security of onshore wind turbines can be compromised by:

- **Security protections**. Sites with weak security measures are vulnerable to theft incidents. Common issues include:
  - ✓ Insufficient perimeter fencing facilitates ease of access to sites.
  - ✓ Lack of, or poor quality, detection security such as Video Surveillance Systems (VSS), movement alarms, etc., means intruders can be undetected or identified.
  - ✓ Lack of intruder alarms can leave turbines with little intrusion deterrence and may delay a security response.
  - ✓ Lightweight padlocks/chains can be easily forced to gain access to the site, turbines and other buildings.
  - ✓ Lack of forensic marking or sprays, and associated deterrence signage.
- **Accessible Routes**. Wind turbines are often located in remote areas but with access from main roads which can enable ease of access and escape.
- **Security Management**. Lack of a security strategy with regards to unauthorised access to and consequential theft from wind turbines.
- **Cyber Security**. Whilst cable theft remains the primary risk, wind turbines are also susceptible to cyber-attacks, particularly where security systems are remotely monitored. Such attacks can compromise critical infrastructure, leading to data breaches, ransomware deployment, and other malicious activities which can cause significant business interruption and are difficult to resolve.

Security Management Plan

Due to the remote locations of onshore windfarms and turbines, a security management plan comprising a number of individual, layered security measures is essential. Such an approach should be designed to deter and hinder unauthorised access, as well as providing suitable warning.

Risk Assessment

Undertaking a Security Risk Assessment helps identify:

- Gaps or omissions in the site management such as ownership, coordination, and communication issues etc.
- The vulnerable assets at the site.
- The likelihood of a theft incident occurring based on sector trends, local knowledge/crime data.
- Anticipated 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 at least annually, or following significant changes at the site, 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 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 specialty in renewables/ wind generation farms or standalone wind turbines 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. Responsibility for oversight of any control measures identified in the risk assessment should be delegated to a responsible person, such as the site manager.

Important: Any planned security protections should be discussed with your Insurer and Broker.

Physical Security

- **Turbine Doors**. For internal door locks, these should be compliant with the BS 3621 series. Any padlocks externally fitted to turbine towers should be in compliance with EN 12320/BS EN 12320: Building hardware. Padlocks and padlock fittings. Requirements and test methods and achieve a CEN grade 5 at minimum. A steel shroud of at least 4mm thickness should be fitted over the padlock to help prevent lock tampering.

- **Security Cage**. Installing a security cage to the entrance of the turbine can delay or deter theft attacks to turbine towers, and should be considered. Security cages should ideally meet the following specification:
  - ✓ **Construction**. Construction of the walls and roof should be of expanded sheet steel mesh of approx. dimensions 3mm thick with 40mm x 85mm mesh size.
    - Ensure the finish is suited for external use, e.g., galvanised, etc.
  - ✓ **Mesh Welded**. The mesh should be welded to a frame made of 40mm x 40mm x 5mm steel angle iron having steel strap cross bracing at 500mm centres through its full height.
  - ✓ **Bolts**. Any bolts joining sections of the cage together are on the inside of the cage and welded to the frame, nut or otherwise deformed to prevent removal.
  - ✓ **Secured**. The cage should be secured to the wall of the turbine and access stairs by good coach bolts quality bolts, 10mm thickness is recommended and at 300mm centres.
  - ✓ **Doors and Locks**. The door of the cage should be of the same construction as the cage, with door hinges of the continuous strip type. At least two hinge bolts are fitted to the hinged side of the door.
  - ✓ **Locks**. The door should be secured by two mortice deadlocks and boxed striking plates certified as meeting BS3621. The striking plates are to be let into the frame and welded in place. Ideally the locks should also be welded in place and to be sited behind a 3mm (min) thick steel plate externally welded to the door and which extends beyond the lock by at least 50mm above, below and away from the closing edge.
  - ✓ **Keys**. Keys should be removed from site.
  - ✓ **Surveillance**. Ensure surveillance cameras are configured to detect out-of-hours tampering of the cage, providing early warning of tampering. Refer Video Surveillance Systems below for more information.

  Note: Any material changes to the turbine access door should be verified with the turbine manufacturer to ensure compatibility and that no product warranties are affected.

- **Cabling**. Spares, high-value cabling, valuable components etc., should not be stored in large quantities at the site during the construction process, and instead delivered to the site 'as needed' to prevent accumulations of theft-attractive equipment.

  If high-value items must be stored overnight, or over several days, additional security measures such as fencing and static deterrence with reactive floodlights and audio challenge should be considered.

- **Site Spares Storage**. Spare stores should be fitted with security shutters, and all door and window openings should be in compliance with local or national regulations, standards or codes.

- **Other Buildings/Compounds**. Lower risk site buildings should feature good quality doors and door locks manufactured in compliance with local or national regulations, standards or codes, and in the United Kingdom complying with 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.

All outdoor equipment cabinets such as externally housed transformers, cable bays etc., should be securely locked, and any switch/control panels also secured to prevent malicious interference.

Refer Aviva Loss Prevention Standards **Security - Doors, Windows and Other Barriers, Security - Glazing** and **Security - Locks** for further guidance.

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 accessible and buried cables and other valuable equipment onsite, allowing any recovered stolen equipment to be returned. Intruder spray systems, which emit a jet of DNA marking solution onto intruders' skin and clothing, are particularly recommended. Pairing with an alarm system and associated deterrence signage is a valuable deterrent against 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.
- Site stakeholders, such as Operations & Management (O&M) teams, should be engaged to ensure that they are cognisant and adequately trained on the use of spray systems to avoid accidental activation.
- DNA marking should also not interfere with normal maintenance activities.
- Backfilling underground cable runs or ducts with cement can reduce the risks of cable theft. A depth of at least 300mm is recommended.
- Aviva Specialist Partner Selectamark provide a range of DNA marking solutions.

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).

- The VSS should be positioned to cover all vehicular points of entry, the customer substation and spares stores, and individual turbines.
- Where there is a suitably near police presence, it would be advantageous to seek to obtain a Level 1 police response, whereby the call will be prioritised for a rapid response. To do so the VSS system would 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.
- VSS should include Automatic Number Plate Recognition (ANPR) equipment to capture and record the registration mark of vehicles entering and leaving the site.
- Temporary mobile video surveillance systems with thermal imaging capability should be added following a site theft incident or to temporarily enhance site security during periods of heightened risk.

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

- 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.

  Refer Aviva Loss Prevention Standard **Video Surveillance Systems - Introduction** for further guidance.

Intruder Alarm

Wind turbine performance monitoring systems, typically known as SCADA systems, provide a degree of security monitoring, certainly should the turbine unexpectedly go 'off-Wind'. Turbine performance monitoring systems, known as SCADA systems, can provide a degree of security monitoring by detecting unexpected interruptions in generation. To do so, owners should consult their SCADA systems provider to set up an alarm specific to unscheduled switchgear operations occurring outside of working hours when personnel are not booked onto site, thus providing a means of intruder detection without the need for installing additional hardware.

Ultimately, purpose-built industry standard intruder alarm protection to the turbines, customer substation and spares units should be considered, particularly where previous thefts have taken place at the location. Any such system should:

- Be designed, installed and maintained in compliance with local or national regulations, standards or codes. In the United Kingdom this is **PD 6662: Scheme for the application of European Standards for intrusion and hold-up alarm systems**, plus the latest version of **BS 8243: Design, installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice**.
- Achieve a system grade of at least Grade 3.
- Achieve a dual path alarm transmission system grading of at least DP3 in accordance with **EN 50136/BS EN 50136: Alarm systems. Alarm transmission systems and equipment - General requirements for alarm transmission systems**, and additionally in the United Kingdom, **PD 6669: Guidance for the provision of Alarm Transmission Systems (ATS) for Alarm Systems in the UK where the turbine(s) are located in the United Kingdom**.
- To help ensure a confirmed alarm activation can be generated early on during any break-in, the system is to provide:
  - ✓ Magnetic alarm contact on the turbine door.
  - ✓ Movement, vibration or glass break detectors.

- The Control and Indicating Equipment/control panel (CIE)) should be sited in an alarm protected area, and intruders should not be able to access it without a high likelihood of a confirmed alarm activation occurring.
- The system should use a means of un-setting that complies with BS 8243 clause 6.4.5. so that any intruders entering the premises via a designated 'entry door' trip a detector and starts the 'entry time', final un-setting to be by Digital Key (fob) - the key reader to be sited just inside the entry door / within the entry lobby.

  Refer Aviva Loss Prevention Standard **Intruder and Hold Up Alarms - General Guidance** for further information.

Security Company Response

Given the remote nature of many wind generation sites, 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 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.

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

Site Access

- All entrance gates and gate posts should 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 shroud of at least 4mm thickness should be fabricated to access gates to help prevent lock tampering.

  Important: Keys for entrance gate padlocks should not be kept on site and any padlock combination codes changed regularly, particularly after staff turnover. 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.
- Large moveable objects such as traffic management boulders or concrete blocks may be used to block disused site routes to reduce the number of access points to the site. However, if any lifting equipment used to transport such objects is left on-site, they should be effectively secured and isolated if necessary to prevent illicit usage.

Perimeter Security

Perimeter security is the first line of defence and also a deterrent to potential intruders, however most wind farms are located in large and remote locations making the installation of good quality security fencing cost-prohibitive and of little practical benefit.

The use of security ditches or terraforming may however help prevent or limit vehicular access to vulnerable perimeter areas, whilst the presence of dense and thorny shrubs or bushes on the perimeter of land near any main roads can provide a deterrent to unauthorised pedestrian access. The use of such measures should be considered within the initial security risk assessment and design stages to ensure planning applications adequately detail proposals.

Other Security

Security guarding should be considered during the initial site construction phases, should high volume of theft attractive cabling be held the site prior to installation, or in the event of repeated 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: 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 strategic use of patrol dogs as part of guarding or site response arrangements is recommended during periods of heightened risk, such as when high value theft-attractive components are left on site overnight. 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.
- Movement activated security lighting can also act as a useful deterrent in some cases, e.g., should persons reside locally or on site who may be able to provide a security alert.

Self-Inspections

Regular recorded inspections of the security protections should be undertaken to check for signs of tampering, damage, cut fencing sections, or unauthorised access. Such inspections should extend to fencing, fencing posts, gates, gate hinges, padlocks, VSS equipment, security signage, locks, 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 integrated with the site planned inspection and maintenance schedule, with an increased frequency during periods of heightened risk.

Security Response Planning

It is important to establish an appropriate Security 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.

Key Action Steps

- Complete a Security Risk Assessment. A registered Security Consultant can assist with this.
- Identify asset and location-specific security protection measures..
- Discuss security plans with your Insurer and Broker.
- Use accredited companies and products.
- Implement a formal security inspection regime.
- Devise a security response plan.
- Routinely test and review security measures and plans, particularly during periods of heightened risk.

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.

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

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

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.
- PD 6662: Scheme for the application of European Standards for intrusion and hold-up alarm systems
- BS 8243: Design, installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions. Code of practice
- BS EN 50131-1: Alarm systems. Intrusion and hold-up systems - System requirements
- BS EN 50136-1: Alarm systems. Alarm transmission systems and equipment - General requirements for alarm transmission systems
- PD 6669: Guidance for the provision of Alarm Transmission Systems (ATS) for Alarm Systems in the UK
- 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.
- Register of Chartered Security Professionals.
- Fire Protection Association RC69 - Risk Control Recommendations for Onshore Wind Turbines

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

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Intruder and Hold Up Alarms - General Guidance**
- **Video Surveillance Systems - Introduction**
- **Unoccupied Premises**
- **Metal Theft**
- **Managing Shutdown Wind Turbines - 12 Top tips**
- **Security - Doors, Windows and Other Barriers**
- **Security - Glazing**
- **Security - Locks**
- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks.**
- **Cyber Security: Respond and Recover.**
- **Cyber Security: The Internet of Things**
- **Ransomware - Cyber Loss Prevention Standard**

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.

26th August 2025

Version 1.1

ARMSGI3292025