



Engineering Report 2

Issue 1 2012

GUIDANCE ON SECURITY OF SUBSTATIONS,
CABLE BRIDGES & CABLE TUNNELS

© 2012 Energy Networks Association

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of Energy Networks Association. Specific enquiries concerning this document should be addressed to:

**Operations Directorate
Energy Networks Association
6th Floor, Dean Bradley House
52 Horseferry Rd
London
SW1P 2AF**

This document has been prepared for use by members of the Energy Networks Association to take account of the conditions which apply to them. Advice should be taken from an appropriately qualified engineer on the suitability of this document for any other purpose.

Guidance on Security of Substations, Cable Bridges & Cable Tunnels

Contents

1. Introduction.....	3
2. Scope	3
3. General objectives of Substation Security Policy.....	3
4. Security Risk assessment	4
5. Assessing Site Vulnerabilities	10
6. Designing Mitigation measures	13
6.1. Site boundary.....	13
6.2. Compound Fencing.....	14
6.3. Intruder detection systems	18
6.4. Perimeter Intruder Detection Systems (PIDS).....	18
6.5. Security lighting	20
6.6. CCTV.....	21
6.7. Manholes / culverts etc	24
6.8. Access control / locking	25
6.9. Windows and Access doors.....	25
6.10. Electric fences.....	26
6.11. Security of earthing	28
6.12. Marking systems and notices	30
7. Routine inspection, records and housekeeping.....	30
8. External interactions on security, and terrorist threat level advice	31
9. Investment plans - Price Control programmes	32
10. Sources of further advice – ref documents, links to web sites.....	32
Appendix A - The main Legal and Regulatory Requirements	34
A1 Electricity Safety Quality and Continuity Regulations	34
A2 Health and Safety at Work Act (1974).....	38
A3 Electricity Act (1989) as amended by the Utilities Act (2000)	38
Appendix B – Example substation assessments	41
B1 Example 1.....	41
B2 Example 2.....	42

PAGE LEFT INTENTIONALLY BLANK

1. Introduction

This Energy Networks Association (ENA) Engineering Report has been developed to provide guidance to electricity network operators in the formulation of policy related to the security measures that may be necessary -

- at substations, to combat enhanced threats from theft and terrorism
- at cable bridges and cable tunnels where there are no parallel specific statutory requirements, to combat enhanced threats from vandalism/trespass, theft and terrorism

This document assumes as a baseline compliance with the ESQCR regulation 3(2) requirement for risk assessment and appropriate measures for substations etc. to prevent danger. It builds upon that requirement to propose a framework for risk assessment and appropriate measures for substations etc. to prevent, so far as is reasonably practicable, interruption of supply. This will help duty holders assure compliance with ESQCR regulation 3(1).

It is of particular relevance to managers responsible for substation, cable bridge and tunnel design and inspection policy.

The Report seeks to bring together expertise held by security experts, networks policy makers and substation designers and to draw upon external sources of reference. It provides a range of available options regarding the design of security arrangements and proposes a risk based approach to substation security management that draws upon the regime of routine site inspection. The Report is not designed to prescribe rigid requirements for particular circumstances or types of installation, but to provide a knowledge-based framework to assist network operators in setting their own policies.

For reference the primary legal and Regulatory issues relating to substation security are summarised in Appendix A.

This Report has been prepared by a task group of electricity distribution and transmission network operator members of ENA and the Security Task Group (STG) under the Energy Emergency Executive Committee (E3C), together with input from DECC and Ofgem.

It is proposed to reconvene a task group in 18 months to two years time in order to review the practical application of the guidance in this document, to establish learning points and revise the document as necessary.

2. Scope

This Report covers additional security design and management techniques for ground mounted transmission and distribution substations, together with high voltage cable tunnels and cable bridges, ranging from over 1,000V up to and including 400,000V, owned and operated by Transmission and Distribution Network Operators.

3. General objectives of Substation Security Policy

The primary objectives to setting policy on substation security are to –

- Provide safety to the general public and children in particular.
- Provide a safe working environment for those authorised to be working in them
- Maintain compliance with legal requirements
- Reduce the risk of theft
- Prevent, so far as is reasonable, loss of supply due to vandalism, theft or terrorism
- Deter, detect and respond to intrusion on a risk assessed basis, noting that a determined person will be able in time to defeat most defences.

In addressing these objectives, Network Operators have to consider proportionality, criticality (of the asset), practicality and expense.

An outline of the legal requirements described in the ESQCRs referred to in Appendix A is:–

- Networks including substations are designed to prevent danger, interference or interruption of supply so far as is reasonably practicable.
- Network operators must assess and record the risk of access/intrusion, having regard to the equipment, the surrounding area and the degree of risk, take commensurate measures to mitigate the risk and review the effectiveness of measures through risk-based routine inspections.

4. Security Risk assessment

In the context of this Report, “risk”, being the product of the probability and consequence of intrusion is essentially two dimensioned; what is the likelihood of a person intruding onto a given site or causing damage to it on one axis and what is the consequence of that in terms of injuries/fatalities of innocent parties or loss of supply to customers on the other.

Persons intentionally defeating basic substation security measures by breaking into enclosures or through or over fences put themselves at risk of fatal accident. Whilst Network Operators may take proportionate measures to deter such intruders, once they have gained access to a site with bare open terminal connections, of greater concern to Network Operators is the risk that innocent children might gain access into a site where security has been breached by others and left unsecured.

In general terms, the national quantities, size of the various types of substation site, and numbers of customers normally supplied is as follows, though Network Operators will have site specific details –

Table 1 – Types of Electricity Substation

Substation Type	Typical Voltage Transformation Levels	Approximate Number	Typical Size	Typical Number of Customers Supplied
Grid	400kV to 132kV	377	250m by 250m	200 000/500 000
	132kV to 33kV	1 000	75m by 75m	50 000/125 000
Primary	33kV to 11kV	4 800	25m by 25m	5 000/30 000
Distribution	11kV to 400/230V	230 000	4m by 5m	1/500

NOTE: The above table is provided to give context to considerations related to the number of customers served by particular network sites. It does not necessarily comprise part of a structured risk assessment process.

Given that larger substations have the greatest volume of assets attractive to thieves, serve the largest numbers of customers and are thus in general more attractive to terrorists, it will normally be the case that these warrant the greater level of security measures. Such a general approach does however have to be tempered with consideration of the nature and use of the surrounding land, or the types of customer and demand being served, such as Critical National Infrastructure (CNI) designated sites or other important infrastructure sites which might elevate the assessed level of risk.

In the case of cable bridges and tunnels the same general approach applies, having regard to the consequence of the loss of multiple assets carried, both in terms of loss of supplies to customers, supply restoration options and costs.

Table 2 below provides some indicative risk scores for typical network sites by class of installation; Network Operators will have a variety of approaches to establishing risk rating for each installation, but they will functionally all cover the same issues.

In risk assessment terminology –

- a hazard is the potential for harm (e.g. some activity or situation) to cause detriment
- a risk is the combination of the likelihood of some form of harm may occur and a measure of the consequence

All substations having open terminal equipment pose a safety risk to the public at large in the event that their security is breached. The levels of security provided to meet statutory requirements having regard both to the nature of the equipment and the use of the surrounding land are designed to provide an appropriate level of safety to the public. The risk ratings set out below in relation to theft and terrorism include consideration of the consequential risk to the public arising from such activity making the site temporarily unsecured.

Cable bridges and tunnels may pose a wide variety of risk; at the lowest level they might involve a single LV cable, whilst in the case of 11kV these might carry the complete output of a 132/11kV substation serving a city centre. They may carry a mixture of different voltage cables, signalling and communication cables. They will not normally house any exposed live conductors.

Ofgem is seeking that network operators utilise a common range of risk scores to facilitate consistent national comparison and, potentially, work programmes. Given that substation sites already meet “ESQCR” Regulation 3 (2) requirements relating to risk of danger, the primary focus of this guidance document is to consider the **additional** risks surrounding potential loss of supply. These “Site Security Risk Index” (SSRI) ratings are then subject to an adjustment through a Public Safety Risk Index to give a reflection of the potential for a consequential additional risk to innocent members of the public entering a site that has been rendered insecure.

For example, thieves seeking to steal live cable from a cable bridge are not likely to leave a dangerous condition for the public because any attempt to remove cable would cause

circuits to trip. Whereas in the case of an open terminal substation, unauthorised access through damaged fencing could lead to danger from exposed conductors.

The risk ratings are illustrated in Table 2 below and range from 1 lowest to 10 highest; network operators could rate sites using a number of parameters, including numbers of customers at risk, nature and use of surrounding land and site history derived from routine ESQCR site inspections.

Whilst Network Operators should make the ultimate determination on how to assess sites to produce risk scores in line with the typical scores in Table 2 an outline of an example procedure is provided below:

1. Sites are assessed for both a site security risk index (SSRI) and a consequential additional public safety risk adjustment index (PSRI)
2. SSRI and PSRI are added for each risk class. The highest scoring of the three risk classes (Vandalism/trespass, Theft, Terrorism) should determine the overall unmitigated risk score for the site.
3. The highest scoring sites (above an appropriate threshold determined by the network operator) should then be subject to a more in-depth site level analysis (e.g. the CARVER approach described below) to determine where appropriate mitigation should be applied within the site.

Under such a process SSRI scores would range from 1-9, whilst PSRI scores would range from 0-2. This disparity is to account for all sites already being ESQCR Regulation 3 (2) compliant, and for the purposes of this assessment it is primarily (although not exclusively) the security of the site from a continuity of supply perspective that is being assessed.

A cable bridge terminating at a DNO substation



Table 2 - Indicative ranges of risk scores for typical network sites

Installation type	Unmitigated Risk Scores						Notes on range of risk
	Vandalism / Trespass		Theft		Terrorism		
	SSRI	PSRI	SSRI	PSRI	SSRI	PSRI	
HV/LV Distribution s/s	Already covered in meeting ESQCR Reg 3 (2) requirements		1-3	0-2	0-1	0-2	In very exceptional circumstances due to nature of customer served, may elevate Terrorism risk. In other circumstances the ESQCR safety requirement will dominate.
Primary 66 or 33/11kV s/s			2-4	1-2	1-2	1-2	In very exceptional circumstances due to nature of customer served, may elevate Terrorism risk
Grid 132/33 132/11kV s/s			2-5	1-2	2-6	1-2	Elevated terrorism risk ranking e.g. resulting from CTSA advice
Supergrid 400/132kV			3-6	1-2	4-8	1-2	Elevated terrorism risk ranking e.g. resulting from CTSA advice
Cable bridge or tunnel 11kV	1-4	0-1	2-4	0-1	1-4	0-1	
Cable bridge or tunnel 66 + 33kV	2-5	0-1	2-5	0-1	2-5	0-1	In very exceptional circumstances due to nature of customer served, may elevate Terrorism risk
Cable bridge or tunnel 132kV	2-6	0-1	2-6	0-1	3-8	0-1	Elevated terrorism risk ranking e.g. resulting from CTSA advice
Cable bridge or tunnel 275+ 400kV	4-8	0-1	4-8	0-1	4-9	0-1	Elevated terrorism risk ranking e.g. resulting from CTSA advice

Note: SSRI = Site security risk index, PSRI = Public safety risk index

The above table represents a range of anticipated scores for typical network sites to facilitate national comparison / discussion. It is recognised that individual companies do employ their own scoring/assessment processes distinct from the table above and if necessary companies should be able to translate their local score to map against the table above.

This process allows an unmitigated risk score to be developed. In accordance with the process for ESQC regulation 3(2) assessments, this score shall be recorded and retained irrespective of any mitigating actions taken. Companies may also record a mitigated score, taking account of the benefits of the measures described later in this document.

This process should:-

- Ensure understanding of the effectiveness of security measures
- Identify the extent of installed security measures and the ongoing need for maintenance and replacement of physical security systems
- Identify the need for investment in additional security, where justified, to reduce the level of risk.

- Ensure a register of sites is maintained recording key information, including prioritised actions for those sites assessed to be at the highest risk.

Note: This process is also applicable for new sites.

The above risk classes are explained in further detail below:-

Vandalism/trespass	
Example SSRI Considerations	Example PSRI Considerations (Already required for substations under Reg 3 (2) of ESQCRs)
Risk to public from loss of electricity supply caused by the above	Risk to the public (children, emergency services) from sites left unsecured by acts of unlawful entry i.e. innocent trespassers)
Indoor or outdoor site	Risk to network operator staff when attending site to operate potentially damaged equipment or repair damage
Numbers and types of customers supplied by the site, particularly if this involves other critical or important national infrastructure.	Nature and use of surrounding/adjacent land (e.g. in a highly or sparsely populated area)
Criticality of site within wider network topography (e.g. number and rating of circuits in a cable bridge)	Previous history of interference or theft
Nature and use of surrounding/adjacent land (e.g. derelict/semi-derelict)	
Previous history of interference or theft	

Because of the factors outlined above typical combined scores for this risk class may span 1-5 for a distribution substation and 4-9 for a major 400kV asset.

Theft	
Example SSRI Considerations	Example PSRI Considerations
Risk to public from loss of electricity supply caused by the above	Risk to the public (children, emergency services) from sites left unsecured by acts of unlawful entry i.e. innocent trespassers)
Scale and attractiveness of assets at the site to thieves	Risk to network operator staff when attending site to operate potentially damaged equipment or repair damage
Criticality of site within wider network topography (e.g. number and rating of circuits in a cable bridge)	
Numbers and types of customers supplied by the site, particularly if this involves other critical or important national infrastructure.	Nature and use of surrounding/adjacent land (e.g. in a highly or sparsely populated area) – see also ESQCR Reg 3 (2) requirements
Nature and use of surrounding/adjacent land (e.g. derelict/semi-derelict)	Previous history of interference or theft
Previous history of interference or theft	

For example, a HV/LV distribution substation scoring 1 indicates a site in a low risk environment, with no history of interference supplying a typical number of customers

whereas a score of 3 would indicate a site in an area of high risk with a history of vandalism and trespass. Because the scale of risk and the attractiveness of larger sites (e.g. a major cable bridge in a large conurbation) higher risk scores will be applicable.

Terrorism	
Note: This does not cover those sites designated as CNI by Government	
Example SSRI Considerations	Example PSRI Considerations
Risk to public from loss of electricity supply caused by the above	Risk to the public (children, emergency services) from sites left unsecured by acts of unlawful entry i.e. innocent trespassers)
Criticality of site within wider network topography (e.g. number and rating of circuits in a cable bridge)	Risk to network operator staff when attending site to operate potentially damaged equipment or repair damage
Numbers and types of customers supplied by the site	
Nature and use of surrounding/adjacent land (e.g. derelict/semi-derelict)	Nature and use of surrounding/adjacent land (e.g. in a highly or sparsely populated area)
Previous history of interference or theft	Previous history of interference or theft

It should be recognised that a terrorist attack on an HV/LV distribution substation is believed to be highly unlikely.

Although not designated, some sites may be more obviously attractive to terrorists than the majority of sites due to their size or the customers/infrastructure/sites they supply.

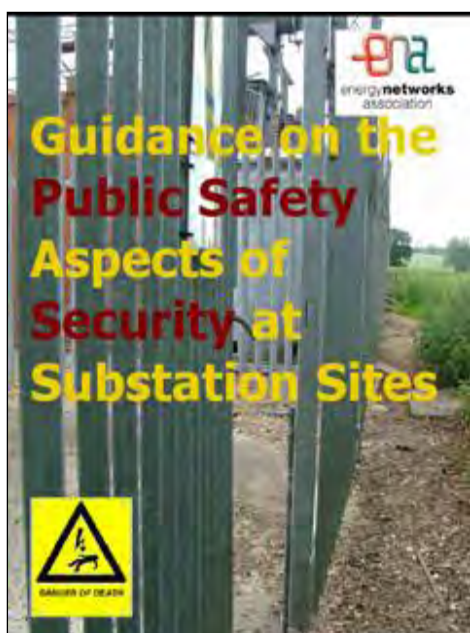
Individual companies may nevertheless wish to carry out assessments of these sites based on some of the risk factors outlined above.

Having established both an SSRI and PSRI modification for a given site a combined risk score can be arrived at. For those sites with elevated scores, the Network Operator would then assess (e.g. use CARVER) site specific vulnerabilities and select mitigation measures from a menu of options.

The Health & Safety Executive publication “Reducing risks, protecting people”, ISBN 0-7176-2151-0 provides helpful guidance in relation to safety risks to people at work and the public in particular, relating to broadly acceptable levels of risk and investment.

5. Assessing Site Vulnerabilities

There are some two hundred and thirty thousand ground mounted Distribution Substations in Great Britain, all of which will have live equipment encased within a metal equipment housing of some sort, or, in the case of open terminal LV switchboards, contained within a larger housing or building. Such substations may be at risk of vandalism, intrusion by children, vagrants or addicts, and by metal thieves seeking to steal the small amounts of copper contained in such substations. The ENA booklet “Guidance on the Public Safety Aspects of Security at Substation Sites” (front cover shown below) is particularly helpful in setting out guidance on public safety vulnerabilities of such sites in a manner suited for use by networks staff undertaking routine substation inspections.



Whilst the above guide also covers Primary and Grid substations, its subject matter is related to public safety and not to the wider context of this Report covering risks arising from loss of supply, theft and terrorism.

It will not be possible to mitigate all vulnerabilities, but a systematic assessment is valuable in identifying vulnerable areas where risk mitigation measures are viable. Such an assessment is based broadly on Criticality, Accessibility, Recognisability, Vulnerability, Effect (impact) and Recoverability (generally termed as “CARVER” Analysis).

- Criticality – how critical is the item to the continuation of the process role of the site (generally to move all the power in to all the power out)?
- How Accessible is the item within the site? What is the site perimeter (e.g. fence) protection. Are there adjacent land uses that elevate risk of intrusion or climb over? Is the item within a further enclosure or building? How secure is that?
- How Recognisable is the item in appearing critical to the site operation? For example a relay room vs. an oil tank or a switch disconnecter?
- How Vulnerable is the item to attack? What would be needed to disrupt the item? Are some parts of it more exposed than others (e.g. a transformer tank housed inside a noise enclosure whilst the radiator banks are located outside. In this example what would happen if oil was lost from the radiator bank?)
- What is the Effect of loss of the items function? Does it disrupt the entire site operation or only one of a number of circuits? How many Customers would lose supply?
- What is the Recoverability from the loss of the item? For example how long would it take for replacement of a piece of copperwork, a circuit breaker, sealing end etc? What is the lead time to obtain replacement equipment and skilled installers? Are spares held?

Having identified site vulnerabilities the next steps are to –

- assess the viability of individual and collective mitigation measures

- to determine the necessary choices of specification having regard to the required function of the mitigation and the interaction with other elements, e.g. in selecting CCTV is the function solely to identify that a human intruder is present, or to be able to identify the intruder to standards that would be admissible in Court? Who will monitor the CCTV? Where? What action will they take etc.?

An approach employed by Government Security bodies is to set out so called “Operational Requirements” (ORs); and formed of a sequence of questions. The Centre for Protection of National Infrastructure (CPNI) publish a “Guide to producing operational requirements for security measures” and the February 2010 version is available for download from the CPNI public view website. Whilst it is not suggested that network operators need to follow the full process, aspects are helpful in highlighting the need to make decisions on elements of specification and use, and extracts have been incorporated into the following section on mitigation measures.

www.cpni.gov.uk

Individual network operators will have a range of approaches to the presentation of policy on adoption of particular types of mitigation measures for different classes of site. From a functional viewpoint some measures will only be viable for some classes of site, and so one approach is the use of a further matrix, possibly linked to risk rating –

Table 4 – Range of mitigation measures generally within scope

	Boundary measures	Enhanced fence	Electric fence	Building alarm	Lighting	CCTV	Windows, doors perimeter	Windows doors in site	Secure manhole	Earth tape security
HV/LV Distribution s/s		√					√			√
Primary 66 or 33/11kV s/s	√	√		√	√		√	√		√
Grid 132/33 132/11kV s/s	√	√	√	√	√	√	√	√		√
Supergrid 400/132kV	√	√	√	√	√	√	√	√		√
Cable bridge or tunnel 11kV							√		√	
Cable bridge / tunnel 66 + 33kV		√					√			
Cable bridge or tunnel 132kV		√		√			√		√	
Cable bridge or tunnel 275 + 400kV		√		√			√		√	

The above table provides an *indication only* of the types of mitigation measures that *might* generally be relevant to higher risk sites. For example, it may not generally be viable to install site CCTV systems on higher risk primary s/s sites, though specific instances might arise where it was.

Whilst Section 6 below indicates a number of mitigation tools available for use on individual existing sites, some have the potential for wider deployment as a deterrent, for example asset marking systems. There may be an opportunity to design other tools into new or replacement installations. Companies may wish to establish liaison with local police forces to

provide supporting information on metal theft in a locality and may also pursue public access campaigns.

6. Designing Mitigation measures

It is important to consider mitigation measures in a holistic manner as there are many interactions between elements, for example –

- Selection of perimeter detection system can be influenced by choice of fence
- Specification of CCTV is influenced by lighting specification, its coverage and the zonal areas of detection systems

6.1. Site boundary

For Distribution substations, the site boundary will normally be coincident with the fence, wall or enclosure boundary. In the case of Primary and Grid substations, the site boundary will often be some distance from the boundary of the live compound. There will be a variety of uses of the land between the two, including -

- Screening with banks or trees as a condition of Planning Consent
- Grazing under licence
- Nature reserve
- Let to third parties e.g. for storage
- Left fallow

Some uses present security challenges with varying degrees of controllability; little can be done in respect of required screening, but controls can be placed on third party use that might provide climbing aids. Such controls might include provision of low level vehicle barriers set away from the fence line or restrictions on storage of drums, planks or other climbing aids in the letting agreement.

Where substation buildings form part of the site boundary it is necessary to assess and mitigate or remove climbing aids and window openings. Access doors on the boundary may warrant a higher specification than some of those within a site e.g. those affording access to non critical areas.



The ENA booklet “Guidance on the Public Safety Aspects of Security at Substation Sites” provides useful advice on the above.

“Defensive planting” is a useful tool in deterring immediate access to compound fences, and there are a range of low level shrubs that can be used requiring limited attention whilst appearing attractive. The following is an extract of information issued by Gloucestershire Constabulary, though many Forces and other bodies provide guidance. In selecting defensive planting it is important to consider speed and final height of planting; for a site boundary tall growing species may be appropriate, but close up to a compound fence low level planting will be needed to preserve sight lines. Consideration has to be given to the means by which the Network Operator will access the outside of the compound fence for inspection and maintenance; that might entail provision of a pedestrian access gate to provide a route from within the compound.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: RUBUS THIBETANUS - Comments: White stemmed Bramble, fern like silvery leaves, pink flowers, clumps of attractive white stems.

Shrub: PYRACANTHA various varieties - Comments: Firethorn, can be kept neat by pruning.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: BERBERIS VERRUCULOSA - Comments: Compact, slow growing shiny green leaves with white undersides, yellow flowers.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: BERBERIS DARWINII - Comments: Bright orange flowers with red tints. A fine flowering shrub.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: BERBERIS BUXIFOLIA - Comments: Orange - yellow flowers, purple grape-like berries.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: CHANOMELES various varieties - Comments: The Japonica or Japanese Quince, saucer-shaped spring flowers can be kept neat by regular pruning.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: HIPPOPHAE RHAMNOIDES - Comments: Sea Buckhorn, white flowers orange berries. Makes a tough hedge.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: ROSA RUGOSA - Comments: Rhamanas Rose, dense prickly stems. Excellent hedging plant.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: CRATAEGUS MONOGYNA - Comments: Common Hawthorn, May or Quickthorn. Makes a superb, wildlife friendly hedge.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

Shrub: ULEX EUROPAEUS PLENA - Comments: Double flowered Gorse, very prickly. Makes a tough hedge.

Flowers	Fruits/Berries	Suitable for walls/fences	Height above 2 metres	Height below 2 metres	Evergreen	Suitable for hedging	OK in partial shade
✓	✓	✓	✓	✓	✓	✓	✓

6.2. Compound Fencing

The minimum legal requirement for all high voltage substation sites having exposed live conductors is a fence or wall of 2.4m height. That height should be measured from a datum representing the highest point that a person could stand, so if a fence is positioned on top of a low wall providing a stepping point, the 2.4m is measured from that datum.

Larger sites at risk of flooding will, in future, increasingly be provided with flood defences and it is necessary to ensure that these do not compromise security of fence lines. In some instances it may be viable to incorporate a new fence into a flood defence wall, providing a dual benefit of inhibiting burrowing intrusion

Whilst some old Primary and Grid sites may have made use of chain link fencing, such installations do not provide the greater levels of security afforded by palisade or certain types of welded mesh fence. Consequently it is appropriate to review the use of chain link against the site risk assessment, intrusion and threat history and condition based need for replacement.

Loss Prevention Standard (LPS) 1175 provides a source for comparison of fencing types each against common criteria and rates them accordingly. Therefore palisade fencing and a welded mesh type fencing having, for example, LPS 1175 level 3 rating will be equally effective in resisting attack. Welded mesh fencing can present a viable alternative where a local authority objects to use of palisade fencing. In the event that such a local authority position presents real difficulty, it may be appropriate to seek support from local Police Security by Design teams or, where relevant and by your Company Security Advisor, Police Counter Terrorism Security Advisors (CTSAs.)

The choice of fencing type interacts with the viability of certain types of perimeter protection system –

- acoustic detection systems do not perform well with palisade fences due to resonance
- conversely, palisades are good where the area to the outside has the potential for human/animal interaction which might give rise to unwanted alarms on such detection systems on welded mesh fences

Modern design of palisade fencing should be in accordance with British Standard 1722 Part 12, though Network Operators should note that it is still necessary to select options from the BS before using this as an enquiry specification. Factors to consider include –

- Height (e.g. standard of 2.4m but may differ on site risk ranking)
- Post centres – e.g. 2.75m
- Maximum spacing of pales centre to centre (e.g. 146mm 18 pales per 2.75m bay)
- Minimum pale face to view (width) e.g. 70mm
- Section and minimum thickness exclusive of finish e.g. 3.9mm “D” or 3.0mm “W”
- Strength testing and deflection tested in accordance with Appendix A of BS 1722 Part 12
- Number of rails (two lower rails provide additional security against prising/jacking apart). A manufacturer might also offer a design having the pales slotted through the rails)
- Riveted or rivet-less design (considered in combination with section (“W” section provides a higher level security than “D”) Rivet-less in turn offering further security
- Pale to rail and post to rail fixings, type and strength – e.g. saddle or T head bolts grade 8.8 with shear head cone nuts There is no British Standard for Shear headed Cone Nuts – a typical requirement might be - Cone nuts to be steel strength grade 8 as detailed in BS 4190 and threaded in accordance with BS 3643.

- Post sections and toppings
- Security of rails to posts – use of welded connector plates
- Protective treatment – e.g. galvanising to BS EN ISO 1461
- Design width and depth of concrete sills and post foundations
- Designs to prevent undermining of fences
- Design of gates, anti lift hinges, locking and bolting systems and avoidance of creation of climbing aids
- Integration of network operator locking arrangements
- Provision for fitment of ancillary electric fencing
- Topping enhancements and fixings such as rotating vanes or razor wire (must be in excess 2.4m)
- Design of wing panels where fence has to meet adjoining fencing such as post and wire cattle fence.
- Means of transitioning between different height ground levels
- Fence earthing connection requirements

Some of the above options may only be available from a single supplier and all will have a cost impact and so a balance will need to be struck. This might entail the highest security design fence only becoming viable on the highest risk or designated sites.

Tensioned Concertina barb tape (razor wire) installed on V top is one of the most effective anti-climb deterrents. Installation is subject to a number of controls –

- No overhang into the public domain unless it is installed at a suitable height so that it cannot be inadvertently touched (2.1m or above)
- Suitable signage which should be visible from any point of approach/access/egress
- It can be fitted at ground level if internally behind a fence within a perimeter; however there would be a duty of care to install a low level demarcation fence and signage as above (having regard to subsequent network operator access to the compound fence line for maintenance and weeding)

An alternative to use of BS 1722-14 outlines welded mesh fence security requirements

There are different grades of such fencing having various rod thickness and spacing and resulting security performance. The same types of specification requirements generally apply as in the above list for palisade, though the positioning of vertical rods should be on the outside of the fence to reduce the climbing aid provided by the horizontal bars, and higher posts than makers standard may be required. There are a number of positive and negative comparisons between use of welded mesh and palisade –

Positive

- improved visibility into site
- Less visually intrusive
- Less easy to cut or prise open providing that suitable section rod is used in the mesh
- Lighter to handle
- climbability

Negative

- Poor durability compared with palisade
- Strength to ram attack
- Reduced ability to use on sloping ground where extreme gradients apply

Palisade supplemented using weldmesh (internal view)

