Insight

# PHYSICAL PERIMETER PROTECTION FOR UTILITIES SITES

Jacksons Fencing

## Sector News

### Utilities

Energy related work is expected to remain a strong potential growth area. The UK is in need of investment into new power generating capacity over the next 5 years, in order to plug the impending supply gaps as aging, inefficient and carbon emitting power stations close.

### Utilities Construction (£ million)

| Region | 12 | 13 | 14 | 15 |
|---|---|---|---|---|
| East Midlands | 99 | 203 | 376 | 246 |
| East of England | 163 | 368 | 472 | 199 |
| London | 113 | 156 | 101 | 52 |
| North East | 50 | 64 | 163 | 92 |
| North West | 62 | 79 | 418 | 227 |
| N. Ireland | 30 | 146 | 289 | 55 |
| Scotland | 222 | 515 | 980 | 279 |
| South East | 61 | 293 | 508 | 132 |
| South West | 104 | 317 | 587 | 132 |
| Wales | 48 | 100 | 386 | 48 |
| West Midlands | 35 | 146 | 216 | 27 |
| Yorkshire/ Humber | 178 | 161 | 436 | 241 |

Source: Glenigan

The combination of high investment in the utility sector, and the need to replace ageing and inefficient power stations to meet renewable energy targets, suggests that physical security specifically designed to address the needs of the industry will rank highly on the business agenda in the foreseeable future.

Companies operating in the utilities sector (including production, treatment, processing, distribution and supply), face the risk of potential security breaches which could have significant implications on public safety and / or service availability.

To date the UK utilities industry has not experienced a major security violation, but there have been a series of incidents, which highlight the vulnerability in this sector.

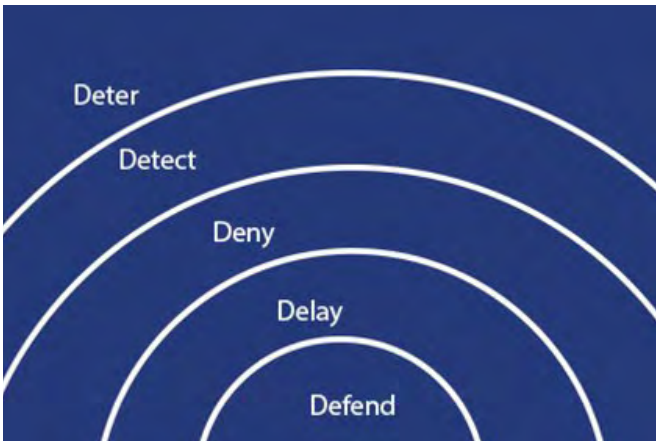
In November 2013, a break-in at a substation in Greenock resulted in a power surge that set four homes ablaze and a further 280 properties being without power. Two years previously 50,000 homes in Glasgow were left with no power following an attempted theft at a substation. In the US, over 150 rounds of ammunition were fired which cut through two critical telecommunication cables to the Pacific Gas and Electric substation in California causing $15 million in damage – an event viewed by some as a 'dress rehearsal' for a much broader attack that would result in widespread power outage; causing renewed thinking to legislation related to the security of national infrastructure.

While the installation of physical security products to protect sites is an obvious critical requirement, for those responsible for procurement comes the burden to correctly specify those products whose design and manufacture have been proven to deliver the security performance, resilience and longevity required in this high risk environment. Equally important is the commitment to ongoing inspection and maintenance of all physical security devices once they are installed to ensure their continued efficacy to ensure they continue to work their design specification.

## Identifying the risk


Following a review of Operational Requirements, usually a two stage process where the requirement for the security of assets is first established before the solutions are identified, a resulting security plan will typically employ the Onion Principle to provide multi-layered protection.

The aim is to work from the outside into the centre, treating each different boundary as a layer which is hardened to delay the attacker, provide greater protection to the target and give security staff the intelligence they need to implement their response.




This methodology of assessing the perimeter security requirements of a site from the perspective of someone attempting to get in is far more realistic and effective than working from a printed plan, a web search, a specification sheet, or a fixed budget from a desk in an office.

## The 5 D Perimeter

There's a lot of discussion around the 5 Ds of effective perimeter security - to detect, deter, delay and deny access in order to defend assets - and perhaps these days, a little too much is centered around electronic detection and surveillance technologies within the broader topic of the 'Internet of Things' and connected devices.

But perimeter security, whether for manned or unmanned remote sites is equally about creating an effective physical barrier which can detect, deter, delay and deny unauthorised access to the protected area and ultimately defend the asset.

A well planned, designed and installed fence and access solution will add real substance to the protection of a perimeter and can also yield significant savings in the overall cost of site security by reducing the requirement for more expensive electronic alternatives or manned guarding.

## Specify for success

Once the threats facing the site have been established and the products designed to mitigate risks and provide the desired level of protection are identified, the focus shifts to selecting the right products from the right suppliers.

For higher risk sites, various tested and approved or certified products designed to mitigate different types of threat are available, which all carry the assurance of proven performance; for example LPS 1175 provides a security rating for products (1 = lowest rating, 8 = highest) based on the attack time a product is able to withstand given an allowable tool set and maximum work time.

Most utilities sites would employ products which have been tested and certified under LPS1175 while for higher risk sites, Approved for UK Government Use products may be recommended by CPNI (The Centre for the Protection of National Infrastructure) as part of their advisory remit.

Where Hostile Vehicle Mitigation measures to protect against vehicle borne attack is required, PAS 68 and IWA 14 certified crash rated fences / barriers / gates provide effective solutions.

## Installing for performance

Any physical perimeter security product, regardless of the testing it has undergone to prove its ability to withstand various challenges is only as good as its installation. It can only deliver to its design specification if it is regularly inspected, maintained and repaired. Therefore, buying decisions need to also consider a number of contributing factors which affect the integrity of these performance critical products.

For example materials employed in their construction should be both fit for purpose and able to deliver a long service life. Any steel used which is exposed to the elements above or below ground should at the very minimum be hot dip galvanised to BS EN 1461, inside and out, and ideally after basic manufacturing has been carried out. The steel wire used in the production of mesh fence panels should be coated with a zinc-aluminum alloy treatment to BS EN 10224 in preference to standard galvanised for increased life expectancy. If timber is used it is good practice to ensure that it is manufactured from the right part of the right species of timber so that it is capable of accepting the required timber treatment which will protect it against rot and wood boring insects. Attention should be paid to fixtures and fittings -tamper evident, single use or integral concealed fixings on fencing and gates are far less vulnerable than nuts, bolts and rivets.




Given that physical perimeter security is an essential part of the infrastructure of a site and crucial to its safe operation, selecting products which are supported by a worthwhile quality guarantee makes a great deal of sense; as along with the peace of mind that comes with having immediate recourse in the event of a product failure, it also ensures costs are contained.

## Maintaining performance

The final element to good physical perimeter security practice is the regular and scheduled inspection of the fence line to identify any changes which could impact on its security integrity. Litter, debris and dirt should be regularly cleared to allow an unhindered view of the condition of the fence and all repairs required identified and remedied in a Condition Report.

Gates, turnstiles, barriers and blockers equally need to be regularly tested and checked for mechanical wear and tear, to not only maintain operational efficiency but also to ensure the continued safety of those entering / exiting the site. Particular attention should be paid to the safe operation of automated gates and barriers, which are classed as machinery and as such, are covered by legislation requiring the occupier of the facility to ensure that they remain in safe working order. It might sound obvious, but just because a product hasn't failed does not necessarily mean that it is working properly.

…and unless there is standard practice in place to routinely inspect, check, test, maintain and repair the physical elements of perimeter security infrastructure, it probably will.

## Contact Us

For further information, advice or to arrange for a site visit, please contact us on +44 (0) 1233 750 393 or email security@jacksons-fencing.co.uk

## Head Office Security and Export Enquiries

Jacksons Fencing
Stowting Common
Ashford
Kent TN25 6BN
United Kingdom

T: +44 (0) 1233 750 393