

“Effective perimeter security; how can you be sure it is effective?”

Richard Flint – Certification Scheme Manager BRE Global Ltd.

The perimeter should provide the first line of defence against unauthorised incursion, whether by personnel or vehicles. It is therefore essential that a site security risk assessment is undertaken to identify any weaknesses and to ensure that processes are put in place to mitigate against the threat of an attack.

In terms of perimeter security, the system should:

- Provide a sufficient delay against incursion by people, allowing time for the attack to be detected and an effective response to be deployed.
- Provide suitable resistance to incursion by a vehicle. This can involve the use of features such as the layout of approaching roadways and natural features, as well as hostile vehicle mitigation (HVM) products, such as bollards and blockers.

The performance of HVM equipment should be rated and approved in accordance with recognised standards, such as PAS 68 (UK), CWA 16221 (Europe) and IWA 14-1 (International). Meanwhile, BRE Global’s Loss Prevention Standard LPS 1175* defines the resistance to manual forced entry provided by perimeter protection, such as fences, gates and turnstiles, as well as that provided by HVM equipment.

The standards for HVM that are commonly specified (e.g. PAS 68) cover the barrier’s resistance to impact by a defined vehicle travelling at a defined velocity in a defined direction. The standards do not account for the vulnerabilities many barriers exhibit in terms of a person’s ability to undermine its resistance to unauthorised incursion by those who attack it using tools in order to allow easier passage by the target vehicle. The very nuts and bolts that provide the maintenance engineer speedy access to critical components can also result in hostile actors being able to rapidly render a HVM system ineffective. Many vehicle barriers are therefore vulnerable to being overcome using basic disassembly tools such as a spanner or socket set, let alone some of the more serious tools many fences and other perimeter barriers are increasingly designed to resist.

However, while a large number of perimeter fencing systems are approved to LPS 1175 and a growing number of gates and turnstiles are undergoing the evaluation and approval process to that standard; no HVM measures have yet been approved to LPS 1175. Why not? And, what are the potential risks faced by those specifying measures that have not been approved?

LPS 1175

A HVM barrier’s resistance to manual attacks is covered within LPS 1175; a standard that is already widely recognised for other elements of perimeter protection as well as barriers commonly forming other layers in a site’s security.



So why aren't any HVM barriers approved to LPS 1175 yet?

Put simply, it is a case of chicken and egg. Many specifiers have not considered the threat and therefore the potential vulnerabilities the equipment they are specifying and using may exhibit. Furthermore, those that do are faced with not having products available to them. Rather than challenge the market to develop it, they tend to stick to asking for what is available rather than remaining focused and being resolute in only specifying what they need. And, despite there being a real need for HVM barriers that offer such resistance to attack, the lack of visible or vocal demand from specifiers for vehicle barriers that provide such resistance to attack means suppliers do not recognise the need to demonstrate their product's resistance to manual attack, and certainly cannot support their arguments to banks and shareholders if they wish to obtain funding for developing products that do provide that performance and independently demonstrate that performance. The other factor that has deterred manufacturers from submitting their products for approval to LPS 1175 is the fear of failure. Why? According to Richard Flint (Physical Security Certification Scheme Manager at BRE Global), 95% of products submitted for evaluation tend to fail to achieve the required performance levels at the first attempt. Most physical security products therefore need to be modified by the manufacturer in order to achieve the delay against manual forced attack the supplier wishes to claim or their clients' are seeking.

Another reason HVM barriers tend not to be approved to standards such as LPS 1175 is the fact that most manufacturers sell their products on the back of type tests rather than backed by independent third party approvals. While many suppliers will give their prospective clients access to a type test report (at best) or a 'certificate of test' (which merely provides a summary of performance achieved by the specimen tested), such evidence does not provide any guarantee the equipment being supplied and installed fully reflects that tested or that it will provide the same levels of performance. Although the product's name may be the same as that on the test evidence and although the product supplied may look like the specimen tested, many unseen differences can exist which affect the products' ability to provide that performance. For example, the materials used to form the product may have changed, or there may have been changes to the way in which the product was welded or otherwise assembled and installed. Therefore, although the tests may have been conducted by a reputable laboratory; such as MIRA and TRL; it is important to realise that a test report only relates to the specimen tested. The report itself, and any associated test certificates, provide limited assurance and will provide very limited protection to those using the product in the event something goes wrong. However, while such changes may be hidden from specifiers, or those inspecting the installed product on their behalf, and may affect the products' ability to deliver the performance claimed, such changes are not hidden from the approvals body issuing the third party approval, unless fraudulently so. Those seeking enhanced assurance that the products specified and installed will deliver the required

performance should therefore insist the products they deploy are covered by valid third party certification and carry an appropriate certification mark such as LPCB.

Not only does specifying third party certificated products help to provide greater assurances the products used will provide the required protection, specifying independently approved products could not be much simpler. BRE Global, who operate the LPCB certification schemes, publish an up-to-date list of approved products and services known as the Red Book. This is available to view in App form as well as online as a searchable database or in pdf format downloadable from the Red Book website (www.redbooklive.com). The listings not only confirm the performance achieved by each certificated product, and to which standards they are certificated, it also defines their scope of certification. In doing so it helps to ensure specifiers are fully informed when making critical specification decisions.

It is important to remember that criminals and terrorists only have to be lucky some of the time, those protecting themselves from criminals and terrorists have to be lucky all of the time. Using HVM barriers that are independently certificated to standards such as CWA 16221, PAS 68 and LPS 1175 will help to ensure those barriers can be relied upon to deliver the protection required rather than taking the gamble that it may be one of the products that fall within the 95% fail rate.

For further information visit www.redbooklive.com or email PhysicalSecurity@bre.co.uk.

**Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers*