

# LEVEL 2 OPERATIONAL REQUIREMENTS FOR HOSTILE VEHICLE MITIGATION MEASURES

OCTOBER 2010

The Level 2 Operational Requirement (OR) for Hostile Vehicle Mitigation (HVM) measures follows on from the Level 1 OR to provide a more detailed picture of the HVM scenario and issues faced. The Level 2 OR can be used to investigate both existing and proposed HVM measures and can highlight specific vulnerabilities that require mitigation or management attention.

---

i. Document references

Location reference / title:
Issue number:
Issue date:
Document reference:

**Protective marking:**

**ii. Level 1 OR references**

Project reference / title:
Issue number:
Issue date:
Document reference:

**iii. Level 2 OR references**

Indicate other Level 2 OR documents being produced in conjunction with this Level 2 OR.

Pedestrian perimeter barrier	Physical delay (building construction)	PIDS (Perimeter Intruder Detection System)	IDS (Intruder Detection System)
Access Control	CCTV	Security lighting	Mail screening & security
Infosec (Information security)			

## Protective marking:

### 1. Area of concern

Identify the boundary or area to be protected. Produce separate Level 2 OR reports for each area of concern.

Area ( <i>describe</i> )	Tick	Existing / Proposed
Wide area perimeter:		
Site perimeter:		
Building threshold:		
Asset protection:		
Vehicle Access Control Point (VACP):		
Emergency access point:		

### 2. Period of Concern

(i.e. describe when the area of concern is at greatest risk).

	:hour(s) / day(s) / week(s)
	:month(s)
	:years(s)

## Protective marking:

### 3. Vulnerabilities

Identify physical features, technology, processes and plans that could make the site vulnerable and explain why they may reduce the effectiveness of HVM security. This work will assist in the development of a security risk assessment. Considerations include:

- Location;
- Existing VSB protection;
- Traffic management;
- Vehicle Access Control Point (VACP);
- Guard-force;
- Procedures & plans.

Location	Tick	Vulnerability/Comment
Land ownership:		
Rights of way:		
Neighbouring properties:		
Distance from critical asset (m):		
Potential hostile vehicle approach routes (e.g. footpaths, cycle paths, grassland areas):		
Critical services (e.g. gas, electric, water, cooling, communication):		
Existing VSB protection	Tick	Vulnerability/Comment
Type of VSB protection:		
Positioning or gaps:		
Hostile vehicle impact rating: If yes, to what standard and rating? If no, describe measures		
Stand-off distance (from protected asset):		

**Protective marking:**

Site vulnerabilities

Traffic management	Tick	Vulnerability/Comment
Traffic inclusion / exclusion:		
Peak flow & traffic volumes:		
Proximity to public highway:		
Queuing traffic:		
Vehicle parking (legitimate or otherwise):		
Accident hot-spots (in close proximity that may affect HVM measures or VACP layouts):		
Vehicle Access Control Point (VACP)	Tick	Vulnerability/Comment
Type (single line, interlock, final denial):		
Identification/verification method (pin code, swipe card, staff pass etc):		
Closure method:		
Emergency override:		
Automatic or manual system:		
Space for queuing vehicles:		
Vehicle rejection capability:		
Vehicle parking / waiting / queuing / pick-up / drop-off zones:		
Search regime (who, what, when, where, why, how):		
Segregation of vehicle and pedestrian traffic:		

**Protective marking:**

Site vulnerabilities

<b>Guard-force</b>	<b>Tick</b>	<b>Vulnerability/Comment</b>
Guard-force presence:		
Armed guard-force:		
Over-watch guard-force:		
Location:		
Protection from blast:		
Protection from duress:		
Duties (control CCTV, access control, search, admin etc):		
Lines of sight (e.g. physical obstruction, weather, vegetation):		
Response to attack:		
<b>Procedures &amp; Plans</b>	<b>Tick</b>	<b>Vulnerability/Comment</b>
Change in threat and security response level plan:		
Emergency procedures and plans:		
Traffic management plan:		
Incident recovery plan:		
Procedural vulnerabilities (identification, search, rejection etc):		

**Protective marking:**

Site vulnerabilities

Identify vulnerabilities in the existing or proposed security systems which will integrate with HVM measures and could compromise security or operational requirements.

Security measure	Tick	Vulnerability/Comment
Pedestrian perimeter barriers:		
Physical delay (building construction):		
PIDS (Perimeter Intruder Detection System):		
IDS (Intruder Detection System):		
Access control:		
CCTV:		
Security lighting:		
Mail screening & security:		
Information security:		
Existing HVM and traffic management measures:		
Other (specify):		

**Protective marking:**

**4. HVM measure(s) function**

Specify the purpose and function of the proposed HVM measure(s). The threat stated in the Level 1 OR as well as the organisations risk appetite will help clarify these functions, be it against suicide vehicle-borne terrorism, robbery, burglary, vandalism or unauthorised access.

<b>Purpose <i>(of proposed HVM measures)</i></b>	<b>Tick</b>	<b>Comment</b>
Deter:		
Delay:		
Disable:		
Stop:		
<b>Function</b>	<b>Tick</b>	<b>Comment</b>
Provide blast stand-off:		
Control vehicle access:		
Mitigate encroachment:		
Mitigate penetrative attack:		
Other (Specify):		



**Protective marking:**

**5. Performance requirements - Modus Operandi**

Identify attack Modus Operandi (MO) to be mitigated

Modus Operandi	Tick
<b>Parked</b> – Vehicle-borne IED (VBIED) in close proximity to the asset or perimeter:	
<b>Encroachment (1)</b> – Hostile vehicle negotiates through gaps in perimeter:	
<b>Encroachment (2)</b> – Surreptitious vehicle tailgate; vehicle follows closely behind a legitimate vehicle whilst a VSB is open:	
<b>Encroachment (3)</b> – Aggressive vehicle tailgate; vehicle forces leading vehicle(s) out of the way and drives through an open VSB:	
<b>Penetrative (1)</b> – Single vehicle; rams through the perimeter or VSB line:	
<b>Penetrative (2)</b> – Sacrificial vehicle; rams through the perimeter or VSB to create a gap for encroachment of a second hostile vehicle:	
<b>Deception (1)</b> – Pretence; vehicle occupants appear to have legitimate access (with or without use of formal identification):	
<b>Deception (2)</b> – False identification / documentation:	
<b>Deception (3)</b> – Trojan vehicle; vehicle either stolen, purchased or modified to match vehicles familiar to site:	
<b>Deception (4)</b> – Unwitting mule; legitimate driver unknowingly delivers an IED or hostile person(s) into site:	
<b>Duress (1)</b> – Guard-force is forced to allow vehicle entry:	
<b>Duress (2)</b> – Driver (legitimate or otherwise) is forced to deliver an IED or hostile person(s) to the site line:	
<b>Insider</b> – Person with legitimate site access facilitates an attack, by either operating or damaging HVM measures:	
<b>Tamper</b> – Barriers are tampered with the aim to operate, circumnavigate, damage or disable:	
<b>Layered attack scenarios</b> – Using two or more of the above attack MO:	

**Protective marking:**

**6. Impact and performance requirement (hostile vehicle)**

State HVM measure(s) performance requirement under vehicle impact conditions

Protection level			
Provide minimum enforceable blast stand-off distance:			m
Hostile vehicle penetration (beyond the rear face of the HVM measure):			m
Maximum allowable dispersal of major debris (beyond the rear face of the HVM measure):			m
The HVM measure's resistance to blast:			
Threat	Tick	Impact angle (°)	Impact speed (km/h)
Motorcycle:			
1,500 kg car [M1]:			
2,500 kg 4x4 pick-up [N1G]:			
3,500 kg Flat bed (RWD) [N1]:			
7,500 kg 2-axle rigid lorry [N2]:			
18,000 kg 2-axle rigid lorry [N3]:			
30,000 kg 4-axle rigid lorry [N3]:			
Construction / plant (specify):			
Military (specify):			
Other (specify):			

**Protective marking:**

**7. Performance requirement (normal operation)**

State how the HVM measure/VACP is to perform under normal site operating conditions. Where possible identify traffic volumes by category.

<b>Legitimate site users</b> <i>(i.e. users allowed inside the secure perimeter)</i>	<b>Tick</b>	<b>Comment</b>
Asset owner:		
Landlord:		
Operator:		
Staff / employees:		
Guard-force:		
Visitors:		
VIPs:		
Post / deliveries:		
Waste disposal:		
Maintenance staff:		
On-site contractors:		
Off-site contractors:		
Taxi drivers:		
Emergency services:		
Other (specify):		

**Protective marking:**

Performance requirement

<b>Legitimate site traffic (i.e. traffic allowed inside the secure perimeter)</b>	<b>Tick</b>
Pedestrian:	
Equestrian:	
Bicycle:	
Motorcycle:	
1,500 kg car [M1]:	
2,500 kg 4x4 pick-up [N1G]:	
3,500 kg flat bed (RWD) [N1]:	
7,500 kg 2-axle rigid lorry [N2]:	
18,000 kg 2-axle rigid lorry [N3]:	
30,000 kg 4-axle rigid lorry [N3]:	
Construction / plant (specify):	
Military (specify):	
Emergency services (specify):	
Other (specify):	
Traffic volumes (time of day, vehicle type, user)	

## Protective marking:

### 8. Physical constraints

Identify any physical constraint that either precludes the use of certain HVM measures or will require additional engineering.

Constraint	Tick	Comment
Topography (e.g. gradient or level changes):		
Ground conditions (e.g. type, condition, structure, load and bearing capacity):		
Foundation depth (useable):		
Underground services or other obstructions:		
Overhead structures (e.g. type and height):		
Future developments (e.g. own or on neighbouring land):		
Deployment / installation / removal (e.g. is there adequate space for heavy equipment on site? Will security be maintained during works?):		
Other (specify):		

**Protective marking:**

**9. Environment constraints**

Describe any significant environmental conditions that may affect the performance or deployment of HVM measures.

Constraint	Tick	Comment
Wind:		
Rainfall:		
Snowfall:		
Temperature range and cycles:		
Daytime hours & natural light levels:		
Water table:		
Drainage & flood risk:		
Local air condition (e.g. acidic, salinity):		
Presence of other matter (e.g. rubbish, foliage, sediment):		
Ground pollution (e.g. fuel, chemical, waste):		
Site of special scientific interest:		
Heritage or archaeological areas:		
Other (specify):		

## Protective marking:

### 10. Rules and regulations

Identify legislation and local regulations that could affect the design, implementation and operation of HVM measures, for example:

- Local authority
- Highways
- Planning
- Sites of Special Scientific Interest (SSSI)
- Site specific

Comment on issues or constraints:

## Protective marking:

### 11. Success criteria

State the success criteria and, if applicable, how the criteria will be measured.

Criteria & method of measurement	Tick
Blast stand-off:	
Mitigation of identified vehicle-borne threat:	
Penetration distance:	
Traffic management:	
Rejection of unauthorised vehicles:	
Health and safety requirements (site specific, regulatory):	
Aesthetics:	
Guard-force assignment instructions are manageable:	
Service Level Agreement established with barrier maintenance company / department:	
Operational reliability (of HVM measures):	
Short and long-term training programme developed for users, operators and technicians:	
Compliance with internal and external regulations, codes of practise and applicable standards:	
Other (specify):	



## Protective marking:

### 12. Integration

State the level of integration required between different security measures/systems.

Security measure	Tick	Comment
Pedestrian perimeter barrier:		
Physical delay(building construction):		
PIDS (Perimeter Intruder Detection System):		
IDS (Intruder Detection Systems):		
Access control:		
CCTV:		
Security lighting:		
Mail screening & security:		
Information security (Infosec):		
Other (specify):		

**Protective marking:**

**13. Management**

Identify specific project management requirements for each of the project phases (planning, construction, installation, commissioning and operation). Name the person responsible (owner) for each area and any specific actions required, such as:

- Clear procedures (e.g. emergency or response to hostile attack)
- Resources (e.g. guard-force or budget)
- Auditing (timetable and actions)
- Training (who and to what level?)
- Risk analysis (e.g. regular review of threat analysis and security vulnerabilities)

Management area	Tick	Owner
Security risk:		
HVM scheme design:		
Planning:		
Installation of HVM measures:		
Commissioning of HVM / VSB:		
Operation:		
Search and screening:		
Emergency procedures:		
Health & safety:		
Training:		
Security auditing:		
Maintenance & repairs:		
Other (specify):		

**Protective marking:**

**14. Service & maintenance**

Specify the level of technical and service support that is required from the equipment provider.

Requirement	Tick
Commissioning & handover: <ul style="list-style-type: none"> <li>• Factory acceptance test</li> <li>• Commissioning</li> <li>• Site acceptance test</li> </ul>	
Documentation: (Generic or as built and installed) <ul style="list-style-type: none"> <li>• Installation drawings</li> <li>• Circuit diagrams</li> <li>• Cable diagrams</li> <li>• Hydraulics / pneumatics diagrams</li> <li>• Control console drawings</li> <li>• PLC / program</li> <li>• Training manual</li> <li>• Training schedule</li> <li>• Training log</li> <li>• Spare parts list</li> <li>• Operation / product certificate</li> <li>• Operation &amp; maintenance manual</li> </ul>	
Maintenance (Based on manufactures recommendations and usage): <ul style="list-style-type: none"> <li>• Preventative - service intervals (time or operational cycles)</li> <li>• Reactive (repair when broken)</li> </ul>	
Service Level Agreement (SLA): <ul style="list-style-type: none"> <li>• Call-out response time</li> <li>• Repair time</li> <li>• Supply and holding of components</li> <li>• Performance indicators</li> <li>• Penalties</li> </ul> <p>Ensure other site specific requirements and legislated regulations are covered and costed in the agreement where applicable, for example:</p> <ul style="list-style-type: none"> <li>• Working at height regulation</li> <li>• Working in confined spaces</li> <li>• Lone worker</li> </ul>	
Warranty period:	
Other (specify)	