

# Forced Entry Standards

A guide to forced entry protection standards for façades and other building elements used within UK.



National Protective  
Security Authority

OFFICIAL



**This guide introduces the most widely  
recognised standards for forced entry  
protection specified in the UK.**

## Introduction

This guide is intended to help security managers and practitioners understand and select the most appropriate standard(s) for a given forced entry threat.

Several standards define how to determine the **delay** façades and other building elements (e.g. doorsets, grilles, shutters, walls and windows) will provide when targeted by intruders using manual force, with or without the aid of tools.

It is important to ensure the standard(s) selected to determine a façade's or other building element's effectiveness are:

- Appropriate and proportionate to the nature of the threat(s) posed, and
- Applicable to the type(s) of product and/or system that may mitigate the forced entry threat(s) faced.

Charts supporting security managers and practitioners attempting to select a standard are included as appendices.



# Selecting a forced entry protection standard

There are four stages to selecting the most appropriate forced entry protection standard:

- 1 Identify the threat
- 2 Select a standard that is specifically relevant to that threat. This requires an understanding of the standards that are available. To assist with this, the National Protective Security Authority (NPSA) has developed a **Forced Entry Standards Threat Matrix**. It will help users select standards appropriate to both the threat and the adversary's objectives ([Appendix A](#))
- 3 Review the scope of the standards identified to determine which of them include the type of façade or other building element being considered. A table summarising the scope of common forced entry protection standards is attached as [Appendix B](#)
- 4 Select the standard most appropriate to the likely adversary types and levels of intent. NPSA has developed a **Standards Comparison Matrix** which compares the principal features of the various standards for manual forced entry ([Appendix C](#)).

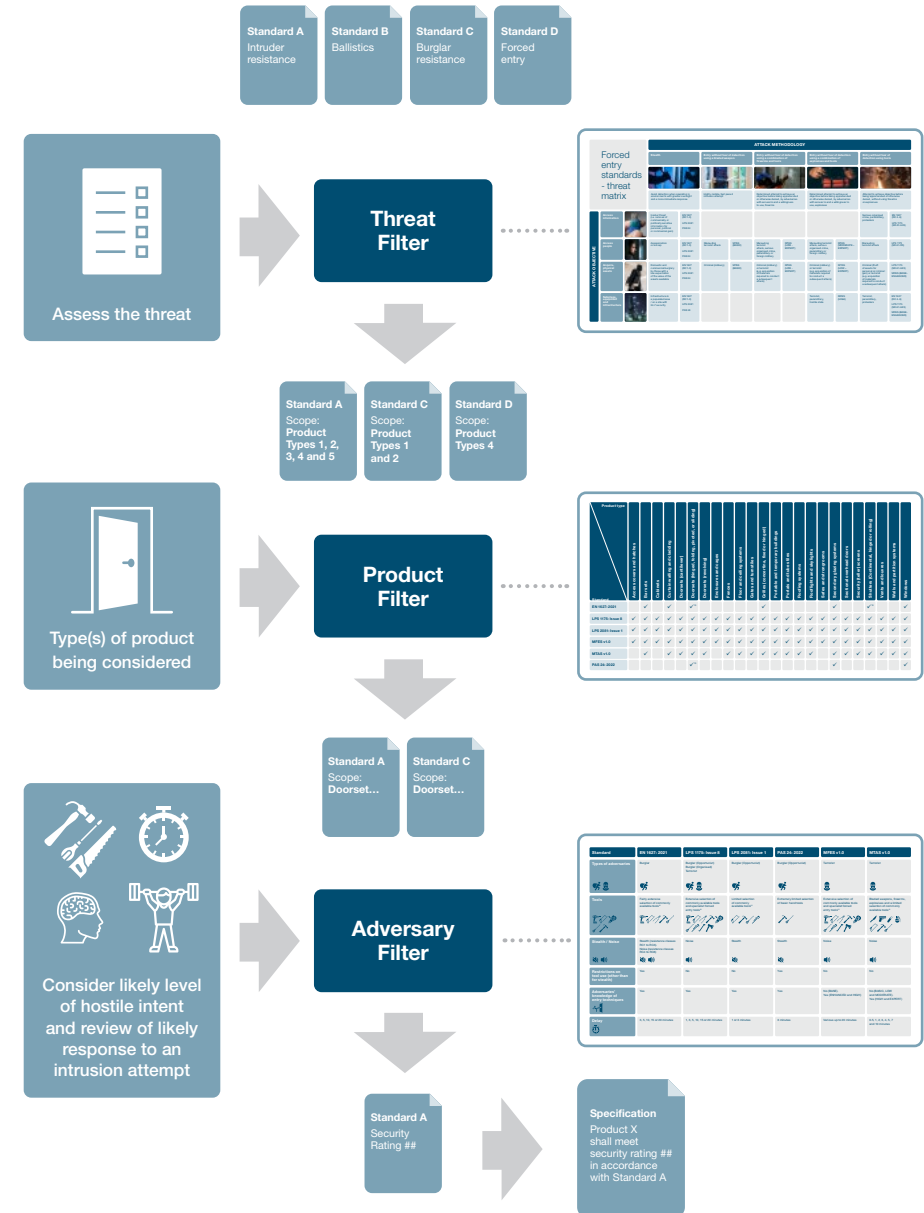


Figure 1: Process for determining which forced entry standard to specify



# Threat

Threat is a product of an adversary's intentions and their capability. Contributing factors include:

- What tools adversaries may use and how they may use them
- How long they may sustain an entry attempt
- How many adversaries may be involved
- How many of those adversaries may use tools during an attempt.

Adversaries will consider what they are likely to require (equipment and knowledge) and do (actions and effort) to maximise the likely success of their forced entry attempt. Their considerations will cover:

## Tools

- The tools they'll need and their skill in using them
- How they will acquire the tools (purchase, borrow or steal)
- How they may conceal the tools during their approach to the target site

## Methods of entry

- The need to minimise the noise they generate during an entry attempt to avoid alerting others (stealth)
- The need to conceal the fact they have achieved entry (e.g. use of surreptitious techniques to support objectives aligned with espionage)
- Concerns about harming themselves during an entry attempt

While none of the standards discussed in this guide consider an adversary's fear of harming themselves, many do consider the size, power and availability of tools an adversary may select. They also consider the potential ease with which those tools may be concealed and transported.



## Features of forced entry performance standards

All the standards covered by this guide are designed to help users determine the resistance a façade or building element will offer to specific types of forced entry.

While most explicitly feature tools, time (delay) and a failure criteria, some allow for variations in the ways adversaries may use tools.

It is not advisable to try and compare one standard directly with another. Each standard considers threats in slightly different ways, and these differences may affect suitability and outcomes.

For example, a product found to provide a minimum delay (say, 5 minutes) when evaluated to one standard may not provide that delay when evaluated to another standard. Given this, it is important to read and understand fully:

- The standard's scope
- The specific performance requirements defined within the standard
- The restrictions noted within a standard.

The following pages explore the different ways six of the most commonly specified standards treat various threat factors (tools, noise considerations, numbers of adversaries and delays), and the influence those different factors may have when products are evaluated to those standards.





## Tool selection

Factors an adversary may consider include a tool's potential effectiveness, concealability, portability, ease of use, cost and availability. There is no one-size-fits-all approach and that is reflected in the different forced entry standards available. Each lists very different types of tool.

Given this, it is important to consider the type(s) of tool deemed to be a threat and whether they are included within the standard and the specific performance classification(s) being considered.

## Tool use

Manual Forced Entry Standard (MFES)<sup>1</sup>, Marauding Terrorist Attack Standard (MTAS) and the Loss Prevention Standard LPS 1175 standard do not restrict how any tools may be used.

However, the EN 1627 standard includes several restrictions on how tools may be used. These restrictions are summarised in [Appendix D](#). Those restrictions do not consider an adversary's freedom, or potential ability, to adapt how they may use a tool depending on their knowledge and experience, or their ingenuity and stamina.

<sup>1</sup> References are contained on page 11.

**Figure 2:** Tools listed in EN 1627 (left), LPS 1175 (centre) and PAS 24 (right)



## Noise

Products generally provide a significantly longer delay to entry attempts involving stealth (i.e, levering and pushing) when compared with the delay they may deliver when targeted by entry methods that generate higher levels of noise (e.g. impacting).

EN 1627 (Performance classifications RC1 to RC3), LPS 2081 and PAS 24<sup>2</sup> focus on the threat posed by adversaries preferring to use ‘stealth’. This should not be confused with ‘surreptitious entry’, which leaves no evidence of an attack.

Other standards, such as EN 1627 (performance classifications RC4 to RC6), LPS 1175, MFES and MTAS permit the use of tools in ways that generate higher levels of noise.

NPSA recommends deploying products meeting one of this latter group of standards if there is any uncertainty regarding whether an adversary may choose to use stealth.

## Number of adversaries likely to use tools during an entry attempt

Table 1 summarises the number of adversaries using tools in a forced entry attack that are provided for by each of the standards.

<sup>2</sup> Product Assessment Specification.

**Table 1:** Number of active adversaries

Standard	Performance classification	Number of active adversaries
EN 1627: 2021	Resistance classes RC1 to RC6	1
LPS 1175: Issue 8	Security ratings A1 to E20	1
	Security ratings F1 to H20	2
LPS 2081: Issue 1	All security ratings	1
MFES v1.0	All protection levels	2
MTAS v1.0	BASIC, LOW and MODERATE performance classifications	1
	HIGH and Expert performance classifications	2
PAS 24: 2022	‘Pass’	1

The standards covered by this guide may not be suited to situations where the threat of more than two adversaries targeting a protective measure is anticipated (e.g. during a riot or protest).

## Knowledge and experience

Most of the standards referred to in this guide assume the adversary has full knowledge of the product and experience using tools.

On the other hand, MFES’s BASE performance classification and the BASIC, LOW and MODERATE classifications defined in MTAS acknowledge adversaries may have limited experience of using tools (e.g. basic DIY skills) and limited or no experience of forced entry techniques.



## Delay

Table 2 summarises minimum forced entry delays represented by each of the performance classifications defined in forced entry standards for perimeter protection products and building components.

**Table 2:** Minimum forced entry delay associated with the performance classifications defined in each standard

Standard	Delay (minutes)									
	0.5	1	2	3	4	5	7	10	15	20
<b>EN 1627: 2021</b>	-	-	-	RC 2	-	RC 3	-	RC 4	RC 5	RC 6
<b>LPS 1175: Issue 8<sup>3</sup></b>	-	SR #1	-	SR #3	-	SR #5	-	SR #10	SR #15	SR #20
<b>LPS 2081: Issue 1</b>	-	SR A	-	SR B	-	-	-	-	-	-
<b>PAS 24: 2022</b>	-	-	-	'Pass'	-	-	-	-	-	-
<b>MFES<sup>4</sup></b>	*0.5	*1	*2	*3	-	*5	-	*10	*15	*20
<b>MTAS v1.0<sup>5</sup></b>	‡0.5	‡1	‡2	‡3	‡4	‡5	‡7	‡10	-	-

<sup>3</sup> # relates to the category of tool used to classify the product's resistance to forced entry (i.e. A to H)

<sup>4</sup> \* relates to the adversaries' level of knowledge and experience (i.e. BASIC, ENHANCED or HIGH)

<sup>5</sup> ‡ relates to the adversaries' level of knowledge and experience (i.e. BASIC, LOW, MODERATE, HIGH and EXPERT).

## Other considerations

While a standard's title may imply the type(s) of products that are covered, its scope should be carefully reviewed to ensure it does actually cover the specific type of products and threats being considered.

Appendices A to C provide a summary of the scope of each standard.

		ATTACK METHODOLOGY					
Forced entry standards - threat matrix		Stealth	Entry without fear of detection using a bladed weapon	Entry without fear of detection using a combination of firearms and tools	Entry without fear of detection using a combination of explosives and tools	Entry without fear of detection using tools	
		Avoid detection when operating in environments with greater oversight and a more immediate response	Highly mobile, fast paced intrusion attempt	Determined attempt to achieve an objective before being apprehended or otherwise deterred, by advancement with weapons to and a willingness to use, firearms	Determined attempt to achieve an objective before being apprehended or otherwise deterred, by advancement with weapons to and a willingness to use, explosives	Attempt to achieve objective before being apprehended or otherwise deterred, without using firearms or explosives	
ATTACK OBJECTIVE	Access information		Insider threat (i.e. removal of commercially or personally sensitive information for personal, political or commercial gain) EN 1627 (RC1-3) LPS 2081 PAS 24			Service impaired crime, paramilitary, professional EN 1627 (RC 4-6) LPS 1175 (SR 4-100)	
	Access people		Assassination or kidnapping EN 1627 (RC1-3) LPS 2081 PAS 24	Mansuering terrorist attack MTAS (BASIC)	Mansuering terrorist attack, without organized crime, paramilitary or foreign military MTAS (LOW - EXPERT)	Mansuering terrorist attack MTAS (MODERATE - EXPERT)	Mansuering terrorist attack LPS 1175 (SR 4-100)
	Acquire, physical assets		Domestic and commercial burglary by those with a low expectation of resistance. High risk of detection if the assets are visible EN 1627 (RC1-3) LPS 2081 PAS 24	Criminal (robbery) MTAS (BASIC)	Criminal (robbery) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack) MTAS (LOW - EXPERT)	Criminal (robbery) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack) MTAS (LOW - EXPERT)	Criminal (both theft of assets for personal or criminal gain) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack) MTAS (BASE-ENHANCING)
	Robbery, equipment and infrastructure		Infrastructure in a populated area with 24/7 security EN 1627 (RC1-3) LPS 2081 PAS 24			Terrorist, paramilitary, hostile state MTAS (BASIC)	Terrorist, paramilitary, hostiles LPS 1175 (SR 4-100) MTAS (BASE-ENHANCING)

Standard	Product type																							
	Access covers and hatches	Barsets	Cabinets	Curtain walling and cladding	Doorsets (cantilever)	Doorsets (hinged, folding, pivoted, or sliding)	Doorsets (revolving)	Enclosures and cages	Fences	Floor and ceiling systems	Gates and turnstiles	Grilles (concealable, fixed or hinged)	Portable and temporary buildings	Portals and tube silos	Roofing systems	Rooftlights and skylights	Safes and strongrooms	Secondary glazing systems	Sectional overhead doors	Security (roller) screens	Shutters (continental, hinged or rolling)	Vents and louvers	Walls and partition systems	Windows
EN 1627: 2021	✓	✓		✓		✓ <sup>10</sup>						✓						✓			✓ <sup>10</sup>			✓
LPS 1175: Issue 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LPS 2081: Issue 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MFES v1.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MTAS v1.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PAS 24: 2022						✓ <sup>10</sup>												✓						

Standard	EN 1627: 2021	LPS 1175: Issue 8	LPS 2081: Issue 1	PAS 24: 2022	MFES v1.0	MTAS v1.0
Types of adversaries	Burglar	Burglar (Opportunistic) Burglar (Organised) Terrorist	Burglar (Opportunistic)	Burglar (Opportunistic)	Terrorist	Terrorist
Tools	Fairly extensive selection of commonly available tools <sup>1)</sup>	Extensive selection of commonly available tools and specialist forced entry tools <sup>1)</sup>	Limited selection of commonly available tools <sup>1)</sup>	Extremely limited selection of basic hand tools	Extensive selection of commonly available tools and specialist forced entry tools <sup>1)</sup>	Bladed weapons, firearms, explosives and a limited selection of commonly available tools <sup>1)</sup>
Stealth / Noise	Stealth (resistance classes RC1 to RC3). Noise (resistance classes RC4 to RC6).	Noise	Stealth	Stealth	Noise	Noise
Restrictions on tool use (other than for stealth)	Yes	No	No	Yes	No	No
Adversaries' knowledge of entry techniques	Yes	Yes	Yes	Yes	No (BASIC). Yes (ENHANCED and HIGH)	No (BASIC, LOW and MODERATE). Yes (HIGH and EXPERT)
Delay	3, 5, 10, 15 or 20 minutes	1, 3, 5, 10, 15 or 20 minutes	1 or 3 minutes	3 minutes	Various up to 20 minutes	0.5, 1, 2, 3, 4, 5, 7 and 10 minutes

## Out of scope

The following are outside the scope of guidance provided in this document:

**Protest:** Although façades and building elements meeting the standards mentioned in this guide may delay forced entry by protestors, none of those standards are specifically intended to determine a product's resistance to manual forced entry by protestors.

Security managers and practitioners concerned about the threat of forced entry by protestors should consider referencing ASTM<sup>6</sup> standard F3038-14 'Standard Test Method for Timed Evaluation of Forced Entry-Resistant Systems'. The test methods defined in this standard are designed to simulate a 'spontaneous mob using readily available hand tools.'

**Surreptitious entry:** None of the standards mentioned in this guide are specifically intended to determine a product's resistance to surreptitious entry.

**Vandalism:** None of the standards explored in this guide specifically address the threat of vandalism of the product being evaluated. In fact, products meeting the standards for forced entry protection described in this guide may be more costly to repair if subjected to vandalism.

For example, security glazing which meets NPSA's MFES standard will deliver elevated levels of protection against forced entry, but its surface is likely to be vulnerable to being cracked or scratched by those wishing to inflict visible damage. That said, protective measures meeting the standards described in this guide will help to prevent a vandal from accessing more valuable or critical assets.

**Components:** None of the standards explored in this guide are specifically related to components, for example, glazing or locks. NPSA advises against specifying standards at component level. This is because doing so can potentially lead to creating contradictory specifications and/or risk specifiers focusing too greatly on components while failing to ensure the assembled product/system provides a suitable global level of protection.

For further information about these threats, contact an NPSA advisor or local Counter Terrorism Security Adviser (CTSA).

<sup>6</sup> American Society for Testing and Measurement ([www.astm.org](http://www.astm.org)).



## References

1. EN 1627: 2021 - Pedestrian doorsets, windows, curtain walling, grilles, and shutters. Burglar resistance. Requirements and classification. BSI<sup>7</sup>, June 2022.
2. F3038-14 - Standard test method for timed evaluation of forced-entry-resistant systems. ASTM, May 2014.
3. LPS 1175: Issue 8 - Requirements and testing procedures for the LPCB<sup>8</sup> certification and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers. BRE Global Limited, January 2019.
4. LPS 2081: Issue 1 - Requirements and testing procedures for the LPCB approval and listing of building components, strongpoints, security enclosures and free-standing barriers offering resistance to intruders attempting to use stealth to gain entry. BRE Global Limited, January 2016.
5. MFES v1.0 Manual Forced Entry Standard. Part 1: Requirements. CPNI<sup>9</sup>, April 2015.
6. MTAS v1.0 Marauding Terrorist Attack Standard. Part 1: Requirements. CPNI, February 2021.
7. PAS 24: 2022 - Enhanced security performance requirements for doorsets and windows in the UK – doorsets and windows intended to offer a level of security suitable for dwellings and other buildings exposed to comparable risk. BSI, October 2022.










<sup>7</sup> British Standards Institute ([www.bsigroup.com](http://www.bsigroup.com))

<sup>8</sup> Loss Prevention Certification Board ([www.redbooklive.com](http://www.redbooklive.com))

<sup>9</sup> Centre for Protection of National Infrastructure. This subsequently evolved to become the NPSA.



# Appendix A – Standards according to attack threat and objectives

		ATTACK METHODOLOGY									
		Stealth	Entry without fear of detection using a bladed weapon	Entry without fear of detection using a combination of firearms and tools	Entry without fear of detection using a combination of explosives and tools	Entry without fear of detection using tools					
Forced entry standards - threat matrix											
		Avoid detection when operating in environments with greater oversight and a more immediate response	Highly mobile, fast paced intrusion attempt	Determined attempt to achieve an objective before being apprehended or otherwise denied, by adversaries with access to and a willingness to use, firearms	Determined attempt to achieve an objective before being apprehended or otherwise denied, by adversaries with access to and a willingness to use, explosives	Attempt to achieve objective before being apprehended or otherwise denied, without using firearms or explosives					
ATTACK OBJECTIVE	Access information	 Insider threat (i.e. removal of commercially or politically sensitive information for personal, political or commercial gain)	EN 1627 (RC1-3) LPS 2081 PAS 24							Serious organised crime, paramilitary, protesters	EN 1627 (RC 4-6) LPS 1175 (SR A1-H20)
	Access people	 Assassination or kidnap	EN 1627 (RC1-3) LPS 2081 PAS 24	Marauding terrorist attack	MTAS (BASIC)	Marauding terrorist attack, serious organised crime, paramilitary or foreign military	MTAS (LOW - EXPERT)	Marauding terrorist attack, serious organised crime, paramilitary or foreign military	MTAS (MODERATE - EXPERT)	Marauding terrorist attack	LPS 1175 (SR A1-D5)
	Acquire, physical assets	 Domestic and commercial burglary by those with a low expectation of the value of the assets available	EN 1627 (RC1-3) LPS 2081 PAS 24	Criminal (robbery)	MTAS (BASIC)	Criminal (robbery) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack)	MTAS (LOW - EXPERT)	Criminal (robbery) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack)	MTAS (LOW - EXPERT)	Criminal (theft of assets for personal or criminal gain) or terrorist (e.g. acquisition of materials required to conduct a subsequent attack)	LPS 1175 (SR A1-H20) MFES (BASE-ENHANCED)
	Sabotage, equipment and infrastructure	 Infrastructure in a populated area / on a site with 24-7 security	EN 1627 (RC1-3) LPS 2081 PAS 24					Terrorist, paramilitary, hostile state	MFES (HIGH)	Terrorist, paramilitary, protesters	EN 1627 (RC 4-6) LPS 1175 (SR A1-H20) MFES (BASE-ENHANCED)


















## Appendix B – Scope of product types covered by each manual forced entry standard

Product type Standard	Access covers and hatches	Bar sets	Cabinets	Curtain walling and cladding	Doorsets (cantilever)	Doorsets (hinged, folding, pivoted, or sliding)	Doorsets (revolving)	Enclosures and cages	Fences	Floor and ceiling systems	Gates and turnstiles	Grilles (concertina, fixed or hinged)	Portable and temporary buildings	Portals and tube stiles	Roofing systems	Rooflights and skylights	Safes and strongrooms	Secondary glazing systems	Sectional overhead doors	Security (teller) screens	Shutters (Continental, hinged or rolling)	Vents and louvres	Walls and partition systems	Windows
EN 1627: 2021		✓		✓		✓ <sup>10</sup>						✓						✓			✓ <sup>10</sup>			✓
LPS 1175: Issue 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LPS 2081: Issue 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MFES v1.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MTAS v1.0		✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
PAS 24: 2022						✓ <sup>10</sup>												✓						✓

<sup>10</sup> Only applicable to doors or shutters protecting pedestrian access routes. PAS 24 and EN 1627 do not cover doors or shutters protecting vehicle access routes, for example, cantilever doors or vehicle access shutters.



## Appendix C – Summary comparison of common forced entry standards used in the UK

Standard	EN 1627: 2021	LPS 1175: Issue 8	LPS 2081: Issue 1	PAS 24: 2022	MFES v1.0	MTAS v1.0
<b>Types of adversaries</b> 	Burglar	Burglar (Opportunist) Burglar (Organised) Terrorist	Burglar (Opportunist)	Burglar (Opportunist)	Terrorist	Terrorist
<b>Tools</b> 	Fairly extensive selection of commonly available tools <sup>11</sup> 	Extensive selection of commonly available tools and specialist forced entry tools <sup>11</sup> 	Limited selection of commonly available tools <sup>11</sup> 	Extremely limited selection of basic hand tools 	Extensive selection of commonly available tools and specialist forced entry tools <sup>11</sup> 	Bladed weapons, firearms, explosives and a limited selection of commonly available tools <sup>11</sup> 
<b>Stealth / Noise</b> 	Stealth (resistance classes RC1 to RC3). Noise (resistance classes RC4 to RC6) 	Noise 	Stealth 	Stealth 	Noise 	Noise 
<b>Restrictions on tool use (other than for stealth)</b>	Yes	No	No	Yes	No	No
<b>Adversaries' knowledge of entry techniques</b> 	Yes	Yes	Yes	Yes	No (BASE). Yes (ENHANCED and HIGH)	No (BASIC, LOW and MODERATE). Yes (HIGH and EXPERT)
<b>Delay</b> 	3, 5, 10, 15 or 20 minutes	1, 3, 5, 10, 15 or 20 minutes	1 or 3 minutes	3 minutes	Various up to 20 minutes	0.5, 1, 2, 3, 4, 5, 7 and 10 minutes

<sup>11</sup> Depends on the performance classification. The selection of tools available increases depending on the performance classification.

## Appendix D – Restrictions on tool use noted in EN 1627

EN 1627 Resistance Class	Restrictions on tool use
RC1	<ul style="list-style-type: none"> <li>No manual attack.</li> </ul>
RC2	<ul style="list-style-type: none"> <li>The rubber hammer can only be used to drive a wedge or screwdriver into an aperture instead of using a hand. It may not be used in combination with any other tool and may not be used to directly impact the product</li> <li>The compass saw, hacksaw and pad saw can only be used to cut grilles and hinges that are accessible prior to the attack commencing. They may not be used to attack any other feature (e.g. dog bolts) or types of products (e.g. to sever the links between punched slots formed in the laths on a roller shutter)</li> <li>The steel tube can only be used on grilles. It may not be attached to a screwdriver or other tools to extend the leverage possible using those tools</li> <li>Glazed elements shall not be directly targeted to create an aperture through which to pass one of the test blocks used to determine if the product has been breached.</li> </ul>
RC3	<ul style="list-style-type: none"> <li>All restrictions noted for tests to RC2 also apply for tests to RC3.</li> <li>The locksmith's hammer can only be used with the pin punches and may not be used to directly impact the product or other tools. For example, the hammer may not be used with a screwdriver to chisel the product or to drive the screwdriver, wedges or a crowbar into gaps within the product to achieve a better purchase.</li> <li>The crowbar may only be used as a lever. It cannot be used as a hammer or axe.</li> </ul>
RC4	<ul style="list-style-type: none"> <li>Glazed elements shall not be directly targeted to create an aperture through which to pass one of the test blocks used to determine if the product has been breached.</li> </ul>
RC5	<ul style="list-style-type: none"> <li>No restrictions on tool use.</li> </ul>
RC6	<ul style="list-style-type: none"> <li>No restrictions on tool use.</li> </ul>

## **Freedom of Information Act (FOIA)**

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

## **Disclaimer**

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2023



National Protective  
Security Authority

OFFICIAL