GUIDELINES ON

FORCED ENTRY PROTECTION

Prepared by:

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

With inputs from:

INTERNAL SECURITY DEPARTMENT
KAWAL SINGAPURA

HTX

Published in June 2026

Table of Content

1. Introduction

Physical attack against security protective barriers using both manual and powered tools poses security concerns in sensitive sites. These tools are portable and effective in cutting through common construction materials.

Forced entry (FE) protection is an essential part of physical security that relies heavily on the use of strong construction materials, systems, and products that are designed to withstand attempted physical break-ins.

To better protect critical assets[1] (CAs) against physical attacks, manufacturers used FE standards to evaluate and develop FE resistant building elements such as door sets, windows, grilles, roller shutters, structural slabs and walls.

This document serves as a guide to the building owners, security practitioners, and Qualified Persons[2] (QPs) responsible for keeping public buildings safe and secure against FE threats.

1 Critical asset refers to any asset within a building that is vital for the building's core functions or operations which should be prioritised for protection, e.g. single point of failures.

2 A Qualified Person (QP) is a registered professional (Architect or Engineer) with a valid practicing certificate, responsible for submitting building plans to Building and Construction Authority, overseeing building works, and ensuring compliance with Singapore's building regulations.

2. Forced Entry Concepts

FE attack is a tactic used to gain illegitimate entry into sensitive areas using a combination of tools that are commonly found in local hardware shops.

The common objectives of FE attacks are to:

a) Gain access to sensitive information,
b) Gain proximity to high value assets or targets, or
c) Sabotage critical equipment and infrastructure

Attacks could be carried out by individuals or groups either through stealth, or using forcible attacks:

a) Gain unauthorised access to a building, room or secured area stealthily without being detected, especially in environments that are subjected to a more immediate security response when being overheard or detected by security technologies. Typically, portable and concealable tools are used to conduct such entry attempts to avoid attention, or

b) Gain illegitimate entry into a building, room or secured area in a forceful manner without the fear of being detected, especially for properties that are located remotely with minimal presence of surveillance. There is a higher tendency to use bulky manual tools and powered tools to perform FE attempts as the level of noise generated is not a concern due to the remote or unsecured environment

Perpetrators could use manual and/or powered cutting or drilling tools to cut and penetrate perimeter fences and vulnerable building elements such as doors, windows, locks/locking systems, structural slabs, walls, fences and ventilation systems etc.

Weak building element(s) could be compromised by FE attacks. For example, partition, dry walls, gypsum or masonry walls, wooden doors, unsecured windows and utility portals and large ventilation shafts are susceptible to FE attacks.

3. Forced Entry Protection Standards

The use of internationally recognised security standards is important when specifying the technical performance requirement of a physical security product.

There are several FE standards worldwide. Different FE standards utilise different testing methodologies, tools and security classifications to reflect the level of resistance (delay time) a product offers.

During the FE certification test, the accredited certification body will carry out carefully planned tests to simulate real-world attack scenarios on the specimen. Based on the operational needs, physical tests will involve varying number of testers emulating novice or experienced adversaries, and evaluating the resistance of specimen's components to a variety of tools and breaching techniques commonly used in overt or covert FE attempts.

Products that have successfully passed the FE tests will then be certified by the certification bodies such as Loss Prevention Certification Board (LPCB), and given a security classification to establish the level of resistance (delay time) that it is expected to perform against a specific toolset.

A certification body may conduct production audits and audit tests to ensure consistent compliance of the product in accordance with the FE standard to provide additional assurance to users.

A certified FE resistant product with a higher security rating will outperform those with lower rating, i.e. better at delaying FE attackers till the arrival of security response units:

a) Proven protection against specified set of FE tools via rigorous testing methods
b) Customised security with a range of resistance levels for different needs
c) Deterrence of criminal activity through visible high-quality FE resistant products such as security door
d) Compliance with industry regulations and security standards
e) Integration with other security detection systems for a layered approach

Building owners should adopt threat-oriented approach when selecting an appropriate FE standard in an objective manner; understand the nature of intrusion threat based on the terrain and operational requirements, security response time as well as the types of detection system used.

Annex A provides a comprehensive list of internationally recognised FE protection standards and guidelines. It is generally not advisable for building owners to compare and benchmark one standard directly with another as each standard considered threats in different ways, i.e. no correlation. These differences may affect suitability, outcomes and choice of protective measures.

The selection of standards is an important process in determining the effectiveness of FE measure against the envisaged threat; the type and number of adversaries, type of tools and method of entry etc.

BRE Global's LPS 1175 standard and the European standard EN 1627 are used as a reference in this guideline for their diverse spectrum of security products that could enhance security in high-risk critical assets in local buildings. To demonstrate that a product delivers its security performance, it would be appropriate for products to be tested and approved to other relevant standards listed in Annex A.

The following table shows the key features of LPS 1175 and EN 1627 standards.

FE Standards	LPS 1175	EN 1627
Geographic Focus	UK (and international users)	European Union (and international users)
Scope	Broad (doors, windows, barriers, fences)	Narrow (building components)
Tools used	See Annex B for an overview of toolsets for LPS 1175 and EN 1627	
Classification / Level of Resistance	Security Ratings[3] (A1 to H20) • A: Low-security environments (e.g. for residential use). • B / C: Medium-security areas (e.g. typical for commercial uses). • D and above: High-security zones	Resistance Classes (RC1 to RC6) • RC1: Low resistance, suitable for areas with minimal threat • RC2–RC3: Moderate resistance, typical for residential use • RC4–RC5: High resistance, for commercial and industrial buildings • RC6: Very high resistance, used in critical infrastructure
Toolsets	Threat-specific, standardised across different security ratings	Standardised across all RC levels
Focus	• Entry without fear of detection when using tools • Supports security layering approach	Stealth / Burglary Resistance
Applications	Residential, commercial, high-security facility	Residential, commercial, high-security facility
Quality Control	• Quality assurance audits for manufacturing process in factories • Certified FE products are listed online in BRE/UK's Red Book live	Factory's internal quality assurance checks

3 The letter in the security rating is referring to the threat level, i.e. toolsets, ranging from A to H. While the number in the security rating denotes the resistance time of the physical barrier which ranges from 1 min to 20 min. For more details on the security rating, please refer to the LPS 1175 standard.

FE resistant products that are tested to a specific standard and performance (level of delay) may differ when subjected to different threat factors (tools, noise considerations and numbers of adversaries) or test standard.

For example, a product found to provide a minimum delay of 5 minutes when evaluated to one standard may not provide the same level of delay when evaluated to another standard as the test methodology and performance criteria vary for each standard. For example, a FE door that is certified to provide a 5 minutes delay against covert FE attacks could not perform well against experienced attackers using heavy or powered tools.

Given this, it is important to understand the test scope of the standard, specific performance requirements and test restrictions. Building owners should also evaluate the overall risk profile of the facility such as security layering, coverage of intrusion detection alarm systems and response time of security units.

4. Applications

Comprehensive security risk assessment should be conducted to evaluate the critical asset's threats, vulnerability and consequences. The enclosure of the critical area requires a consistent level of protection where the FE resistance of the structure and security products are equivalent. Vulnerable adjacent structures, e.g. dry partition walls or false ceilings, unsecured window glass panels, larger unsecured ventilation shafts and openings, which could be breached by manual tools, such as sledgehammer, should carry out structural enhancement works in tandem with the implementation of certified FE resistant products to achieve a consistent level of protection against FE attack.

The weakest component will always be targeted during FE attacks. Hence, in the implementation of FE protection measures, ancillary building elements should also be designed to provide similar levels of FE resistance against the selected test standard and toolset.

The effectiveness of FE protection measures can be improved with security layering approach and complementary security measures such as intrusion detection systems and stringent access control processes. It is important to note that the lack of intrusion detection systems at FE protected areas will result in vulnerabilities that could be detrimental to the successful implementation of FE protection strategies. For example, undetected adversary could carry out sabotages to the CAs without intervention from the security force whom are not being alerted due to lack of an effective intrusion detection system.

To meet the intended security objectives, this could be achieved by enhancing the CCTV coverage, access control measures, and intrusion detection systems in the secured zones. Consequently, the need for FE protection measures may be significantly reduced or potentially eliminated. Details on security enhancement measures can be found in MHA's Guidelines to Enhancing Building Security.

Building owners and security consultants should consider and assess the need for FE protection for high-risk facilities (refer to Annex C for Forced Entry Protection Requirements in High-Risk Facilities, and Annex D for Risk Assessment Approach).

Buildings undergoing security enhancement works could refer to Annex E for the best practices in enhancing building security against FE threats.

A list of commonly asked questions for the design, implementation and use of certified list is included in Annex F.

5. Compliance to Statutory Requirements

The Security and Blast Consultants are required to work with the QP to ensure that the security measures do not contravene prevailing statutory requirements, codes or guidelines published by Government Authorities. If special exemption or approval must be sought from any Government Authority, including SCDF's Fire Safety Department (FSD), to implement any certified FE resistant products, the Security and Blast Consultants shall obtain the necessary approvals from the relevant authorities.

Building owners shall consult SCDF FSD early to ensure that proposed certified FE resistant products meet fire safety requirements stated in the Fire Code.

6. Installation and Certification

The FE resistant products should be installed by qualified professionals who are familiar with the standard, and can ensure that the certified products are supplied and installed correctly.

Installation of the doors, gates, and other security features at all critical entry points (main entrances, loading bays, side doors, windows) must be implemented in accordance with original equipment manufacturer (OEM)'s specifications and method of installation.

After installation, the user should inspect and test the FE resistant products to ensure that the certified FE resistant doors, gates, barriers and systems function as expected; robustness of locks, hinges, frames, and security seals etc.

Building owners should ensure that the FE resistant products are sourced from the certified manufacturers. Test certifications or reports issued by the relevant certification body shall be provided to confirm that the certified product has met the required performance and technical specifications.

7. Maintenance and Inspection

Set up a maintenance schedule to inspect the condition of FE resistant products regularly. This includes checking for wear and tear, ensuring that locks, hinges, and security features are functioning properly.

Certified FE resistant products shall undergo regular maintenance in accordance with the manufacturer's recommendations to ensure continued performance and reliability. In addition, systems that are infrequently used or operated shall be subjected to periodic functional testing to verify that they remain operational and capable of meeting the intended security and operational requirements. Regular maintenance is particularly critical for installations located in areas with high usage frequency of exposure to extreme environmental conditions.

Keep records of the installation, maintenance, and inspection of certified FE resistant products, as this documentation may be required for regulatory purposes.

8. Staff Training and Awareness

Staff Training: Train all personnel in the functionality of the security products, detection systems, emergency procedures, and the importance of maintaining the integrity of the perimeter or building security.

Awareness of Security Protocols: Ensure all personnel are aware of the procedures to follow in the event of an attempted break-in, including how to respond to alarm triggers or suspicious activities.

9. Review and Update Security Measures

The building owner should conduct periodic reviews of the building's security measures to ensure that security equipment and fixtures continue to meet evolving threat levels, and that the building's security infrastructure remains up to date.

If the threats change or building's requirements shift (e.g. due to changes in operations, occupancy or value of assets), it is timely to consider reviewing security features or use of certified FE resistant products to maintain a high protection standard.

10. References

a) NPSA Forced Entry Standards (UK)
www.npsa.gov.uk/protection-forced-entry

b) LPS 1175 Issue 8.2
storage.redbooklive.com/media/assets/LPS_1175_Issue_8_2_Intruder_Resistance_Standard_518a3b21c9.pdf

c) LPS 1673 Issue 1
storage.redbooklive.com/media/assets/LPS_1673_Issue_1_d20dadda68.pdf

d) LPCB Redbook Live
www.redbooklive.com

e) BS EN 1627:2021
Pedestrian door sets, windows, curtain walling, grilles and shutters – Burglar resistance – Requirements and classification

f) BS EN 1628:2021
Pedestrian door sets, windows, curtain walling, grilles and shutters – Burglar resistance – Test method for the determination of resistance under static loading

g) BS EN 1629:2021
Pedestrian door sets, windows, curtain walling, grilles and shutters – Burglar resistance – Test method for the determination of resistance under dynamic loading

h) BS EN 1630:2021:2021
Pedestrian door sets, windows, curtain walling, grilles and shutters – Burglar resistance – Test method for the determination of resistance to manual burglary attempts

i) Guidelines for Enhancing Building Security in Singapore (GEBSS)
www.go.gov.sg/gebss

j) Fire Code 2023
www.scdf.gov.sg/fire-safety-services-listing/fire-code-2023

Annex A – Forced Entry Standards and Guidelines

As the scope, limitations and consideration for threat scenarios vary among the international standards, direct comparison of the standards should be refrained as these differences may affect suitability and outcomes. For example, a product is found to provide a minimum delay (e.g. 5 minutes) when evaluated to one standard, it may not provide the same delay when evaluated to another standard. Hence, it is important to understand the scope of standard, specific performance requirements and restrictions defined within the standard.

For more details on the FE standards, building owners may procure the latest test standard(s) from your designated national standards organisations.

LPS 1175

LPS 1175 standard, developed by LPCB (part of BRE Global) in the UK, sets rigorous performance criteria for a range of security products, including doors, windows, gates, barriers, and other physical deterrents. The standard involves a series of tests that simulate real-world attack scenarios executed by skilled and knowledgeable attackers, and assessing the products' resistance to a variety of tools and techniques commonly used in overt FE attempts.

The test involves a maximum of two adversaries and eight tool categories (i.e. A-H), which include a diverse range of impact, prying and powered tools. Refer to Annex B for an overview of toolsets.

LPS 1175 certified products such as doors, windows and fences are implemented in high-risk facilities and government facilities, commercial buildings and retailers.

Every security product that has passed and certified to LPS 1175 standard is registered in the Redbook Live, an LPCB's online database which lists the suppliers and their FE tested security products. LPS 1175 Issue 8.2 offers 48 different combinations of threat levels and delay times, which provides a wider range of risk levels in terms of attack tools and resistance time. This is a useful reference for building owners sourcing for tested and certified FE resistant products.

BS EN 1627 - 1630

BS EN 1627, BS EN 1628, BS EN 1629 and BS EN 1630 standards are part of a series of European standards that focus on the FE resistance of the windows, doors and other building components.

EN 1627 outlines the requirements and classification for windows, doors, and other building components with respect to FE, particularly with burglary intent. It evaluates the performance of the security products against a range of attack scenarios using various tools and techniques, simulating realistic break-in attempts.

EN 1628 defines the test method for determination of resistance to static loading, which assesses how the product withstands the forces applied to it.

EN 1629 defines the test method for determining the resistance to FE protection measures against dynamic loading. The test involves simulating forceful impacts to break a security barrier such as door or window.

EN 1630 defines the test method for resistance to manual burglary attempts, which simulates a burglar using tools and force to gain entry. It assesses the elements of test specimen against attempts of forced opening.

The test involves one adversary in an area of attack for each test. The range of tools defined in EN 1627 are mostly burglary tools, i.e. majority manual tools and some powered tools.

The performance requirements defined in EN 1628, EN 1629 and EN 1630 must be met in order to classify a product's burglary resistance in accordance with EN 1627.

EN 1627 certified products are commonly used in the following contexts:

Common Use Case (Non-exhaustive)	Security Products (Non-exhaustive)	Description
Government Facilities	Door, window, grilles	To secure government buildings and facilities from unauthorised intrusion
Financial Institution	Door, window, grilles	To protect assets from unauthorised access
Commercial and Retail Security	Door, window, shutter	To protect business and retail stores from burglary
Residential Protection	Door, window	To provide enhanced security protection against break-ins and crime

ASTM F3038-14

ASTM F3038-14 is an American standard that specifies test method for timed evaluation of FE resistant product i.e. windows, doors, walls, grilles and other similar products. It evaluates the performance of these products against low level FE attack from unskilled or opportunistic burglary or mob attack using readily available hand tools as primary threat.

The tests would be carried out by six adversaries. Each adversary can select any tools from the range of manual toolset defined within the standard to maximize the chance in failing the test specimen.

Specimens are rated according to their time FE resistance against four levels of attack, ranging from 5 minutes, 15 minutes, 30 minutes and 60 minutes.

UL 608

UL 608 is a standard that covers the requirements for vault doors and modular steel panels intended for use in financial institutions, commercial, and industrial facilities to protect the assets from burglary attack.

The test involves two skilled adversaries where they could select any common hand tools, picking tools, mechanical or portable electric tools as defined within the standard.

The ratings are based on the length of time which the specimen withstands the attack by the toolsets defined within the standard are as follows:

a) Class M – ¼ hour
b) Class 1 – ½ hour
c) Class 2 – 1 hour
d) Class 3 – 2 hours

Annex B – Overview of EN 1627 and LPS 1175 Toolsets[4]

An overview of toolsets for EN 1627 and LPS 1175 standards.

Manual Toolsets	
LPS 1175 Issue 8.2	**EN 1627:2021**
Pliers Knife Screwdriver and Spanners Wood and Plastic Wedges Crowbar Axe Bolt Cutter Club, Sledgehammer Compass, Pad, Hacksaw Hooligan Bar	Pliers Knife Screwdriver and Spanners Wood and Plastic Wedges Crowbar Axe Bolt Cutter Club, Spalling Hammer Compass, Pad, Hacksaw

Powered Toolsets and Others	
LPS 1175 Issue 8.2	**EN 1627:2021**
Cordless Drill Electric Jigsaw, Circular Saw, Disc Grinder, Petrol Grinder Oxy-fuel Torch	Cordless Drill, Electric Drill Electric Sabre Saw, Jigsaw Electric Angle Grinder

Manual Tools

Manual tools are commonly hand-held tools that require only manual manipulation and human strength as the source of power. These tools could achieve deformation, breakage, disassembly, spalling and removal of the components. Manual tools are used by intruders to manipulate the operable components (i.e. pry open a locked door) and/or breach the fixed components at joints or edges (i.e. break metal mesh away from the anchors). Manual tools can be used in combination with other tools. For example, a bolt cutter can sever the steel rebar after the concrete cover has been broken apart with sledgehammer.

4 For a complete and detailed list of toolsets, refer to the individual standards for more information. Building owners should always take reference to the latest revision of the standard.

Powered Tools

Powered tools are electrically powered by battery or petrol fuel, which can achieve breakage, deformation, material weakening and spalling of the physical barriers. The use of powered tools typically raises the level of detection as noise, vibration, motion, smoke and debris are generated during the attack. Many of the powered tools are heavier and bulkier, hence an adequate amount of space and skills are required to operate the tools effectively.

Thermal Tools

Thermal tools, such as oxyacetylene torch, generate flames capable of burning through steel and concrete. Such tools are used to execute swift cut through materials such as reinforced concrete. Similarly, thermal tools are heavy and require a high level of skill to operate effectively.

Annex C – Forced Entry Protection Requirements in High-Risk Facilities

Building owner should work closely with QPs, and security and blast consultants to optimise the site layout for security and operational requirements. The design of the site layout should minimise the attractiveness for FE:

a) Establish a well-defined perimeter fence to demarcate the boundary
b) Provide intrusion detection system (IDS) at the facility's perimeter to detect unauthorised entry
c) Provide only one personnel entry control point and one vehicle entry control point into the facility
d) Provide multiple layers of protection for the critical assets to be stored
e) Ensure the walls, structural slabs and physical security barriers meet the equivalent FE resistance for the defence layer
f) Eliminate potential hiding places for intruders and provide surveillance system to monitor unauthorised entry

Perimeter fence is effective in defining a boundary and helps in deterring unauthorised access. An effective perimeter fence should have a minimum height of 2.4m which includes the top guard and a minimum footing depth of 300mm to delay tunneling attempt. The aperture of the fence fabric must be able to resist handhold, foothold and cutting with tools. For facility that requires higher level of protection, certified FE resistant perimeter fence can be deployed to mitigate FE attempt by adversary. Perimeter fences also serve an important role in the earlier detection of FE attempt when complemented with fence intrusion detection system (FIDS).

The entrances and gates along the perimeter fence facilitate controlled access for authorised vehicles and personnel. As they are components of the perimeter line, entrances and gates should provide the equivalent level of deterrence as perimeter fence to ensure effective FE protection at the outermost defence layer of the facility.

The structural components of the building, i.e. walls, structural slabs, should provide adequate physical resistance as it can be exposed to FE attempt where the adversary may gain access to the space above or below the CA room. The penetration delay time for an upward attack on the ceiling (floor of upper level) will be longer than the same attack on a wall. While a downward attack on the floor (ceiling of the lower level), the penetration delay time will be shorter for a similar attack on a wall. Therefore, the construction of the structural components should be designed to provide the required delay time where applicable.

The building owner should conduct a comprehensive risk assessment to determine if the CAs or sensitive areas are vulnerable to FE attacks based on a suitable FE standard and toolsets, e.g. LPS 1175 or EN 1627.

CAs with good security layering will have lower risks of intrusion, theft, and vandalism. However, the entrances/exits could be vulnerable to the threat of FE attacks when the adversary could breach the door and access the CA directly. The building owner and security consultant must assess the FE resistance of the CA's door set system and adjacent structural components against the risk of FE.

For comprehensive assessment, the building owner should consider the FE protection needs based on the following guidelines:

a) Risk assessment analysis shall be conducted for the CA rooms' entrances and exits, including walls and unsecured openings, and CA rooms that are adjacent to publicly accessible areas

b) Provide the design specifications of the walls, structural slabs, door and locking systems with details on FE resistance features:

   i. Door of CA rooms should be minimally certified to LPS 1175, EN 1627 or equivalent. Assessment should be conducted to determine the resistance time (of the certified door) and consider alternative solutions if unable to comply to the standard

   ii. Adjacent wall(s) should meet the minimum requirements for 150 mm thick reinforced concrete wall for CA rooms

   iii. Security grilles should be used to secure utility openings (e.g. ventilations shafts, manholes etc.)

   iv. Window openings at CA rooms should be minimised and secured

Annex D – Forced Entry Risk Assessment Approach

Risk Assessment

Focus on single threat scenario of unauthorised entry/FE on CA's ingress and egress points.

When conducting risk assessment for unauthorised entry[5] and FE[6] , the following factors should be considered:

a) Security in depth. Each layer will provide its respective resistance and delay time. However, adversaries can still penetrate layers of security measures with tools eventually
b) Number of layers of security barriers before arriving at the CA rooms, e.g. CA rooms at level 1 with less security layering have higher risk
c) Facilities with a large perimeter have higher risk as in-situ security team may require longer time for interception, e.g. facilities with large land size
d) Facilities without perimeter fence and accessible by members of public may have higher risk, e.g. common public corridors in tenanted buildings or mixed-used developments
e) Facilities without security screening may result in ease of tools being brought into the facility by adversary to carry out FE

As threat derives from an adversary's intentions and their capability, building owners and security professionals should consider the following factors:

a) Number of adversaries that may be involved
b) Tools that may be used by adversaries (i.e. availability of tools, knowledge and capability in using the tools)
c) Method of entry (i.e. overt versus covert entry)
d) Duration of the FE attempt (i.e. resistance time at each security layer)

With a better understanding of the risk profile, the building owner and their security department/ consultants could then select the most appropriate FE protection standard that matches the threat considerations highlighted in Chapter 1. The minimum delay time required for individual CA will also have to be determined based on the envisaged security response time and detection capabilities.

5 Unauthorised entry refers to the act of gaining access to a building, facility, or secured area without permission or legal authority.
6 FE refers to the act of gaining unauthorised access to a building, facility, or secured area by using physical force to bypass doors, windows or other barriers.

To achieve effective defence layers, a comprehensive detection system and physical delay must work collectively to protect the CA from FE attempt. FE needs to be detected so that the security force can intercept to neutralize the threat before CA is being compromised. As the security force needs time to respond to the incident, the required delay time should be greater than the minimum possible response time. Hence, the selection of the FE resistance level of the security product will be determined by the response time of the security force.

Residual Risk(s)

For locations where FE protection cannot be implemented due to site or operational constraints, the building owner should acknowledge the residual risk(s) associated with unauthorised entry/ FE.

Building owners could consider enhancing existing operational or technological measures to minimise and manage the identified risks, e.g. security SOPs, business continuity plans etc.

Alternative Protective Measures

Equivalent FE resistant products should be considered if the product certified to the selected FE standard cannot be implemented due to site constraints, e.g. retrofitting a security door to an existing wall structure that is unable to support the security door.

There are several methods to reduce the risk of FE attacks; physical, operational and technological measures. Building owners can consider the following measures to enhance the protection of the high-risk facilities:

a) Physical measures
   i) 45mm thick hollow core metal doors with high security locks certified to EN 12320, or equivalent
   ii) Expanded metal mesh of 4.5mm minimum thickness with openings that are not larger than 22mm (short way of design) by 57mm (long way of design) to reinforce weak wall structures

b) Operational measures
   i) Enhanced security screenings (e.g. Perform background checks on employees and contractors, conduct a pre-clearance for visitors)
   ii) Visitor management (e.g. Implement a robust visitor management system where visitors are required to sign in/register and be escorted while on premises)
   iii) Training and awareness programs (e.g. Well equipped with knowledge in security protocols, emergency procedures)
   iv) Regular security audits and risk assessments (e.g. Red teaming)

c) Security technology measures

i) Video surveillance system (e.g. CCTVs)

ii) Intrusion detection system (e.g. Passive infrared sensors)

iii) Access control system (e.g. Two-factor authentication, biometric recognition)

iv) Fence intrusion detection system

Annex E – Best Practices

Security Doors

The function of a security door in physical security is to provide a barrier at a point of entry or exit. Door should open towards the likely direction of the threat.

Door frame is an important component of the security door system. Its resistance against FE is essential for ensuring the overall effectiveness of the security door system as it provides the structural support required to secure the door leaf.

Single leaf door provides better security than a double leaf door due to the existing gap between the double leaf that could be exploited by the adversary during a FE attempt (e.g. pry open with wrench or pry bar). Enhancement should be considered to minimise gap on the double leaf door (e.g. welding of astragal in between the door leaf).

Hinges should be protected on the threat side as it could be exploited by intruders to gain unauthorised access. Door hinges could be protected with the following:

a) Installing hinges with non-removable pins
b) Spot-welding the heads of the pins to the hinge plate of each hinge
c) Installing at least 2 hinge-bolts, i.e. near the top and base of the door, to protrude into the door frame when the door is closed
d) Installing a locking pin in the hinge plate

Locking device of the security door is a critical component in keeping the door secured. It should have the same level of resistance as the other door components to resist against FE attack.

The security door for CA rooms should be certified to FE standard which provides robust frame, hinges and locking system, etc.

Avoid using glass sliding doors, glass folding doors and doors with vision panel as the glass components can be easily broken, i.e. higher FE vulnerability.

Window

Window is one of the vulnerable components of the buildings that could be exploited by adversary to gain unauthorised entry. Where possible, the windows should be minimised, especially at CA rooms.

Windows that are easily accessible, especially for CA rooms that are situated on Level 1, should be installed with FE resistant security barrier or system i.e. expanded metal mesh, metal grilles and bars with appropriate delay timing.

Structural Systems

The reinforced concrete (RC) wall enveloping the CA should be at least 150 mm thick RC with high concrete strength and yield stress. Ideally, it should have at least one layer of steel reinforcement bars for enhanced FE resistance.

The RC structural slabs should be constructed with similar properties shared in the above paragraph.

Miscellaneous Openings

Windows and ventilation openings within the CA room should be minimised as these potential gaps could be exploited for unauthorised entry.

Utility openings, such as ducts, vents, pipes, sewers or tunnels, that are located at the boundary fence, building perimeter and CA rooms should be less than man-passable size to deny entry. Adversary can circumvent the existing IDS via these passages and bypass without being detected. For openings in CA room, it should be situated as close as possible to the concrete ceiling slab.

Openings that have a cross-section area of 620cm² or greater (with smallest dimension being more than 150mm if the opening is rectangular, or the diameter being more than 250mm if the opening is circular) shall be secured with grilles made up of vertical rigid steel bars.

Other Protection Requirements

FE, ballistic and blast requirements often go hand in hand when protecting building in high-risk environments.

A FE resistant door could be designed to withstand FE attempts and ballistic attacks to stop bullets from various firearms and resist breaching attempts with tools and force for a specified time.

Similarly, the FE resistant door could be designed to withstand both FE attempts and explosive blast loading against IED threats.

Annex F – Frequently Asked Questions

General Understanding

a) What is a FE standard?

A FE standard is a set of guidelines and testing procedures used to evaluate the resistance of physical security products (like doors, windows, and barriers) against attempts to gain unauthorized access using physical force and tools.

b) What is a certified FE resistant product?

A certified FE resistant product is a building component tested and certified to resist specific attack tools and techniques as defined by FE standards like LPS 1175, EN 1630 or equivalent standards. These building components such as FE doors are designed to delay or prevent unauthorized access during a break-in attempt.

c) What types of attacks can a certified FE resistant product withstand?

The toolsets used are different for each FE standards. It is important that the user study the FE standards before deciding on the FE standard or toolset that matches the building's threat environment. Briefly, based on the standard:

- LPS 1175: Resists attacks using specific tools, categorized into 8 security ratings (A to H). Higher ratings withstand more sophisticated tools for longer durations of up to 20 minutes.
- EN 1627: Focuses on manual burglary attempts and defines resistance classes (RC1 to RC6) based on tools and attack durations ranging from 3 to 20 minutes.

d) How does certified FE resistant door differ from a regular door in terms of security?

Certified FE resistant door undergoes rigorous testing to withstand attacks using tools ranging from basic hand tools to more advanced mechanical or powered tools, based on specific threat levels. Regular doors are not tested to these standards and would fail under similar conditions.

e) Do these doors come with reinforced frames and locking systems?

Yes. Reinforced door frames and multi-point locking systems are integral to certified FE resistant doors to ensure the whole system meets the required security standard.

f) Are these doors effective against other threats, such as fire or ballistic attacks?

The FE standards focus solely on FE resistance. However, products can be dual certified to address fire resistance (e.g. BS 476 or EN 1363) or ballistic resistance (e.g. UL 752 or EN 1522).

g) Why should I consider installing a certified FE resistant door in my home or business?

These doors provide enhanced protection against burglary, vandalism, and targeted attacks, significantly reducing the risk of unauthorised entry. They are ideal for high-risk environments, such as homes in unsafe areas or businesses with valuable assets.

h) How do LPS 1175 and EN 1627 differ?

LPS 1175 focuses on simulating a wide range of attack scenarios and tools with graded security ratings (e.g., A1–D10), while EN 1630 evaluates resistance against manual attacks and uses resistance classes (RC1–RC6). LPS 1175 is widely used in the UK, whereas EN 1627 is a European standard.

i) Why should I use products certified to FE standards?

Certified products provide proven resistance to physical attacks and improve overall security.

j) What types of products are covered under FE standards?

They cover a wide range of security products, including doors, windows, shutters, barriers, locks, fences, and enclosures.

k) Are these standards mandatory for all buildings?

They are not mandatory for all buildings, but they may be required for high-risk critical areas of specific sectors, such as government facilities, critical infrastructure, or high-risk environments.

Design and Aesthetics

a) Do certified FE resistant doors come in various styles and finishes?

Yes, many manufacturers offer a wide range of styles, finishes, and materials to match aesthetics without compromising security.

b) Can I customise the design to match the aesthetics of my property?

Customisation is often possible, but it may affect costs and lead times. Ensure the customisation does not compromise certification.

c) Are there options for glass panels in certified FE resistant doors?

Yes, but glass must be security-rated (e.g. laminated or polycarbonate) and meet the same certification as the door (e.g. LPS 1270 and EN 356 for glazing).

Practicality and Everyday Use

a) Are these doors easy to use for everyday purposes?

Yes, modern designs balance security and usability, offering smooth operation for daily use.

b) Do they provide convenience and accessibility, such as smart lock integration?

Many certified doors can integrate smart locks and access control systems for enhanced convenience and security.

c) What happens in case of a lockout or if the locking mechanism fails?

Emergency access mechanisms are often built in. Ensure you have a backup key or access to a trusted locksmith familiar with the certified locking system.

Alternatives and Complementary Measures

a) Can a certified FE resistant door work with other security measures, like surveillance cameras or alarms?

Absolutely. Combining a certified door with surveillance, alarms, and other physical security measures enhances overall protection.

b) Are there alternatives if I cannot implement a certified FE resistant door?

Reinforcing existing doors with security bars, strike plates, and higher-grade locks can provide a cost-effective improvement, however the level of protection would not be equivalent to doors that meet certification standards. Hence, there is a risk where such doors may be less effective against FE attempt which needs to be accepted.

c) Does the door deter intruders, or is it mainly a delay mechanism?

Certified doors act as a significant deterrent and delay mechanism, often making intruders abandon their attempts.

Certification and Compliance

a) How are products tested under these standards?

Products are subjected to controlled attack scenarios using defined tools, methods, and time limits to assess their resistance.

b) What do the Security Ratings (SRs) or Resistance Classes (RCs) mean?

SRs and RCs indicate the product's resistance level, with higher ratings offering greater resistance to sophisticated attacks.

c) Can uncertified products still provide adequate protection?

While some uncertified products may offer basic protection, they lack the rigorous testing and assurance of certified products, making them less reliable.

d) Do these standards comply with local and international regulations?

Yes, LPS 1175 and EN 1627 are widely recognized and often align with national and international security requirements.

e) How often are these standards updated?

Standards are updated periodically to address emerging threats, new tools, and advancements in security technology.

f) What certifications or standards should I look for in a certified FE resistant product?

Look for certifications like LPS 1175 or EN 1627, depending on your specific threat environment and regional requirements.

Implementation

a) Can a certified FE resistant door be installed in any type of building?

Yes, but the building structure must be robust enough to support the certified door system. Certified installers can ensure compatibility.

b) Can these doors be retrofitted into existing door frames?

In most cases, retrofitting is possible, but the existing frame must meet the required strength and structural integrity standards. Otherwise, the frame may need reinforcement or replacement.

c) How do I choose the right FE standard for my building?

Conduct a risk assessment to identify potential threats and select a standard and security rating that meets your building's specific security needs.

d) Which security rating or resistance class is appropriate for my property?

Low-risk areas may require lower ratings (e.g. B3 or RC2), while high-risk areas need higher ratings (e.g. D10 or RC5).

e) Can I mix products with different certification levels in one building?

Yes, as long as they align with the risk level of the specific area. For example, public zones may have lower ratings, while secure zones require higher ratings.

f) Are these products suitable for residential, commercial, and industrial applications?

Yes, they are versatile and can be tailored to fit different environments, from homes to high-security facilities.

g) Does it require special installation techniques or professional installers?

Yes. To maintain certification and performance, professional installation by certified personnel is essential. Improper installation can compromise security.

Maintenance and Testing

a) Do certified products require regular maintenance?

Yes, regular maintenance is necessary to ensure they retain their performance and comply with certification standards.

b) How do I verify if a product remains compliant after installation?

Conduct regular inspections and testing to check for wear, damage, or tampering.

c) What happens if a certified product is damaged or modified?

Damage or modifications can void the certification. It's essential to repair or replace the product with certified components via OEM.

d) What kind of maintenance is required to ensure the door remains effective?

Regular inspections of hinges, locks, and the frame are necessary. Follow manufacturer guidelines to maintain certification validity.

e) How long do certified products typically last?

Their lifespan depends on usage, environmental conditions, and maintenance, but high-quality certified products are designed for durability.

Cost and Benefits

a) Are certified products more expensive than non-certified ones?

Yes, they may have a higher upfront cost, but they offer better durability, reliability, and long-term value.

b) What is the return on investment (ROI) of using certified products?

ROI comes from reduced risk and reduced losses related to theft or damage.

Security Concerns

a) Can certified FE resistant products stop all types of FE attacks?

Certified FE resistant products are not designed to stop all types of FE attacks, but certified products could significantly delay entry, giving time for detection and response.

b) Do these products also offer protection against ballistic threats or fire?

Not necessarily; separate certifications (e.g., ballistic or fire ratings) are required for those threats.

c) What other security measures should I use alongside certified products?

Consider integrating alarms, surveillance, access control systems, and trained security personnel for layered protection.

Standards Evolution

a) How do FE standards keep up with evolving threats?

Standards are updated regularly to incorporate new testing methods and address emerging attack techniques.

b) Are there any future trends in FE certification?

Trends include the integration of smart technology, sustainability, and enhanced testing for new attack tools and methods.

c) What role does technology (e.g. smart locks) play in certified security systems?

Smart locks and IoT-enabled devices can complement physical security by adding layers of digital control and monitoring, though they must also be robust against cyber threats.

Legal and Regulatory Considerations

a) Are there building codes or local regulations regarding certified FE resistant doors?

Building owners and QP should refer to the prevailing BCA and SCDF regulation. Some high-risk areas or facilities (e.g., government buildings) may mandate certified doors.