CFPA EUROPE®

GUIDELINES

SECURITY GUIDELINES FOR MUSEUMS AND SHOWROOMS

CFPA-E®-Guidelines 05 : 2012/S

Foreword

The Security Commission of the Confederation of Fire Protection Association Europe (CFPA-E) has developed common guidelines in order to achieve similar interpretation in the European countries and to give examples of acceptable solutions, concepts and models. The CFPA-E has the aim to facilitate and support fire protection and security aspects across Europe.

The market imposes new demands for quality and safety. Today fire protection and security aspects form an integral part of a modern strategy for survival and competitiveness.

The guidelines are primarily intended for the public. They are also aimed at the rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help increase fire safety and security in society.

These guidelines have been compiled by the Guidelines Commission and are adopted by all fire associations in the CFPA-E.

These guidelines reflect best practice developed by the countries of CFPA-E. Where the guidelines and national requirements conflict, national requirements must apply.

Content

1 Introduction

Museums and showrooms are places of aesthetic visualisation of cultural creativity that serve as trustees of our cultural heritage. As sites that collect, preserve, exhibit and explain art and culture, they often house unique objects, either on a permanent or temporary basis, many of which are irreplaceable and extremely valuable.

Museums and showrooms therefore have a special responsibility: they need to protect the “objects d’art” and collectors’ items entrusted to them from a plethora of risks in the best possible manner.

This applies to smaller as well as bigger museums. The document has been designed to be particularly useful for smaller or medium size museums and private collections. However, most of the content of this guidance document is applicable to museums and collections of all sizes. These Security Guidelines can also be used as reference during the planning stage of a building to help both the architect as well as the museum executive responsible for security and safety of the objects.

In order to meet their special responsibility, a museum’s management needs to implement a systematic protection scheme that clearly defines and documents the necessary structural protection measures as well as the organisational safeguards. Such a protection scheme would typically include a specific risk assessment from which it derives protection concepts against identified risks.

Organisational measures in the context of the protection concept such as access restrictions, bag searches and adequate surveillance “top off” the protection concept to be developed against burglary and theft, by also preventing any pick pocketing or acts of vandalism during opening hours. However, visitors’ legitimate interest in inconspicuous and discreet checks must always be taken into consideration.

Electronic and optical systems should complement mechanical safeguards to monitor the areas structurally protected, and to activate an alarm in case of a crime (burglary or lock-in). The further outside electronic safeguards are deployed (e.g. as perimeter protection with, say, alarm loops in the outer glazing), the faster an alarm is triggered, causing immediate intervention by security guards if connected to the police or security services (cf. Figure 1-1). In addition a mere perimeter safeguards, “trap protection monitoring” should also be incorporated to detect locked-in burglars as early as possible.

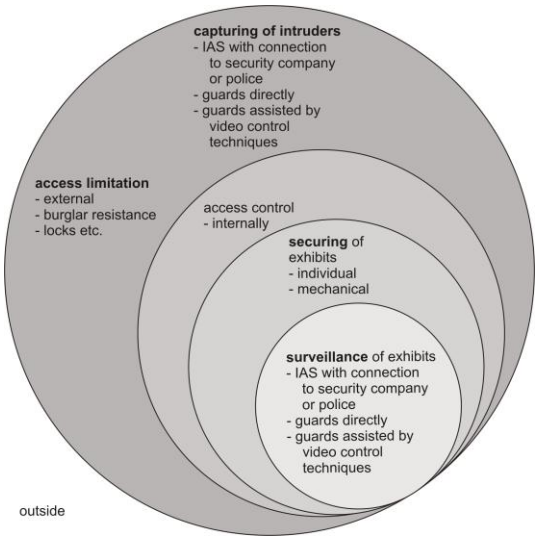

Figure 1-1 Defence-in-depth principle

These Security Guidelines provide practical recommendations to protect museums and showrooms against the risks of

- burglary
- theft by visitors or employees
- robbery
- vandalism
- fire, smoke and radiant heat
- damage by natural hazards and water.

Experience shows that approved physical security elements (as e.g. windows and doors) installed in the course of the erection of a building provide the most effective protection. Often, mechanical upgrades do not provide the same level of protection, though they clearly enhance security. In this context, planners, users and security officers need to focus their attention on the weakest elements of the security chain and, if required, upgrade them.

The general recommendation is to protect and/or monitor an object at risk with both mechanical and electronic safeguards. Manned security and surveillance and the overall organisation of different protection measures are important components of an optimum protection concept.

The most important prerequisite for the different safeguards is to complement one another in a useful way and constitute a harmonised security chain that makes it possible to insure the museum. The Security Guidelines take up these principles and provide recommendations on how to install such a security chain. Hence, users should always review individual safeguards and determine whether they weaken or strengthen the security chain.

The top priority of a risk assessment for a museum or cultural institution is personal safety. This applies in particular to risks such as fire, robbery and threats to visitors by terrorist attacks which are a risk to be increasingly taken into account, particularly in the case of exhibitions that have political or religious themes.

Protection of the building is secondary to personal safety which, in case of a fire, might have adverse effects on the building if priority is given to open escape routes. However, the best possible coordination of personal safety and asset protection measures involving the police and fire brigade ensures a high level of protection for artefacts and collectors' items.

Hence, the optimum protection concept against burglary/theft takes into account the structural measures that provide optimum protection as early as the design or planning stage to refurbish a museum or its storage and restoration workshops (see Figure 1-2).

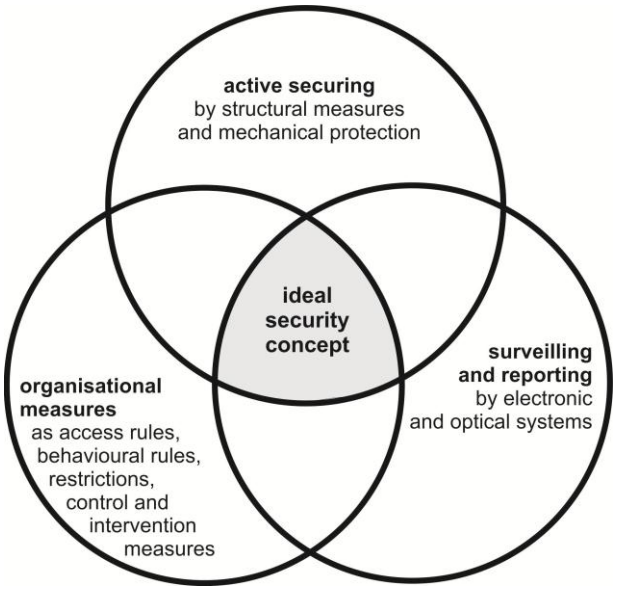

Figure 1-2 Active protection

Mechanical safeguards such as burglary resistant windows and doors play an essential part. Good mechanical safeguards feature robust burglar resistance – the higher the resistance, the harder it becomes for the burglar to overcome these safeguards (in terms of time, tools, expertise) – which increases the risk for the perpetrator to be discovered and caught.

When coordinating mechanical and electronic safeguards, the most important aspect is adequate burglar resistance of the mechanical safeguards. As the perpetrator would need more time to overcome the safeguards, it becomes more likely for security guards who have been alerted to intervene in time. It also helps to prevent successful "smash and grab" break-ins that European museums are increasingly affected by.

The objective of these Security Guidelines is therefore to make operators and supporters of museums, security officers, planners and the police aware of the various options of security technology with a view to burglary/theft, fire protection and protection from natural hazards and water damage in museums and showrooms. They provide non-binding recommendations to parties involved for developing an effective protection concept (structural/organisational/electronic) against the risks outlined here.

These Guidelines do not cover measures for protection against any other risks which include e.g. light, climate, insect infestation or improper handling of objects by museum staff or the development of contingency plans.

Regarding the development of contingency plans, further national references may be considered useful (as the German document "Creation of Evacuation and Rescuing Plans for Art and Art Work", Erstellung von Evakuierungs- und Rettungsplänen für Kunst und Kulturgut, VdS 3434).

These Security Guidelines explicitly take into consideration that every building has different structural and organisational properties, e.g. requirements for the conservation of historical buildings or the composition of staff.

The scope of protection therefore always needs to be tailored to the individual organisation, the respective value of the artefacts and collectors' items as well as their type and size.

A classification of the museums in terms of the required scope of protection can only be made to a limited extent and is not subject of these Security Guidelines.

In general, every facility has different occupancies and premises at risk. Therefore, it is useful to establish protected zones depending on the relevant occupancy. Protected zones can be enclosed buildings, parts of buildings or rooms that are enclosed and that house the objects to be monitored. Protected zones may be independent or dependent of one another (cf. chapter 3.2.4).

Protected zones independent of one another may be useful, among other things, to prevent mutual damage in case of different occupancies (e.g. conversion of an exhibition area, operating a restoration workshop independent of opening hours, third party occupancy managing a café). This makes it possible to protect certain parts while others are being used.

The Guidelines also address:

- Taking objects d'art out of storage
- Tracing ownership
- Transport
- Outdoor exhibitions
- Short exhibitions (e.g. in savings banks, financial institutions, authorities, administrations and large trading corporations)

Implementation of protection measures

When implementing protection measures, different intentions, skills and motivations of perpetrators and their expected approaches and the level of surveillance at different times need to be taken into consideration.

Listed buildings need to comply with special requirements. Mechanical safeguards as well as intruder alarm systems (IAS) might impact the structure, e.g. by requiring changes to doors, windows, walls, ceilings and floors. It might, for example, be necessary to install an visual warning device (e.g. strobe light) to protect and/or preserve assets, which might contrast with conservation principles for historical buildings and/or aesthetic considerations. This is why officials from conservation authorities for historical buildings should be involved as early as possible to find a solution that ensures effective burglary protection while also taking into consideration principles of architecture, art and conservation. Often, innovative security solutions can be developed through cooperation with officials of conservation authorities that take into account the respective local conditions. Depending on the scope of the measures, conservation permits might be required.

Where certified and approved burglar-resistant elements are installed (e.g. burglar-resistant doors, security upgrades installed by experts on windows etc.), all parties involved can be certain that these products proved during intensive tests that they are well suited as protection against burglaries. For instance, a certified burglar-resistant door needs to withstand an attack with tools typically used for a break-in for a defined minimum time. In general, the resistance level of a safeguard – resistance that a safeguard poses to an attacker – needs to be adequate. The higher the resistance level, the longer a perpetrator needs to enter a building or steal an object – the greater the chances that intervention forces, e.g. the police, will succeed in preventing the crime, catching the perpetrator in the act or prompt him to abort his project altogether.

In general, products for burglary and theft protection are divided into different classes. Investigations by the police show that many attempts at a burglary fail because of sophisticated security technology. The perpetrator needs to try harder the more sophisticated the protection; he loses time to overcome the safeguards which may prevent him from completing the theft.

Important note: When planning, installing and operating the protection measures, the relevant legal provisions and requirements for escape and evacuation routes must be complied with. More detailed provisions are contained in the respective regional building codes. Moreover, requirements for fire protection and protection from damage caused by water need to be taken into account.

2 Risks

Although the level of threat differs from one museum to the next, there are nevertheless comparable basic risks to which almost all museums are exposed. The level of exposure of museums and showrooms is determined by a number of factors such as location, size, type of exhibits (in particular material values of collections, cultural heritage and damage for which there is no material compensation) and political/religious relevance etc.

In order to assess the risks, an individual protection concept has to be developed.

The **protection concept** generally represents an analysis of possible attack and loss scenarios (taking into account potential damage) aimed at achieving a defined protection level. In this context, it is important to distinguish protection against malicious attacks (*security*) and protection from human or technical error (*safety*).

All protection concepts have a structural approach in common:

- Defining the object to be protected and protection goals
- Assessing the likelihood of a loss and potential scope of damage
- Analysing the threats/damage scenarios
- Developing measures to reduce the likelihood /scope of a loss
- Planning measures and providing means to prevent and mitigate the loss if the risk materialises
- Analysing degree of risk that can be tolerated
- Even a sophisticated protection concept is not able to completely eliminate the residual risk.

Above all it is important to consider that the security arrangements may need to be modified quickly if personnel with direct responsibility “on the ground” recognise a developing problem requiring a swift and practical solution, compatible with the overall strategy.

One of the main problems in practical and operational risk management is a realistic assessment of risks, which is often based on subjective assumptions, and the identification of useful early warning indicators to monitor risk potential.

The risk assessment includes the determination of probability of occurrence and the possible scope of damage. It is based on a structured approach that classifies the risk and provides insight into the factors that have a positive or negative influence on the risk. The greater the probability and scope of damage, the more the project is at risk and the more the need for it to be radically rescheduled. Different methods can be used for the risk assessment.

Benefits of a comprehensive risk management: potential problems and exposures, can be identified at an early stage.

Pitfalls of risk management: despite good research, risks can only be estimated. Such estimates always imply a certain degree of uncertainty.

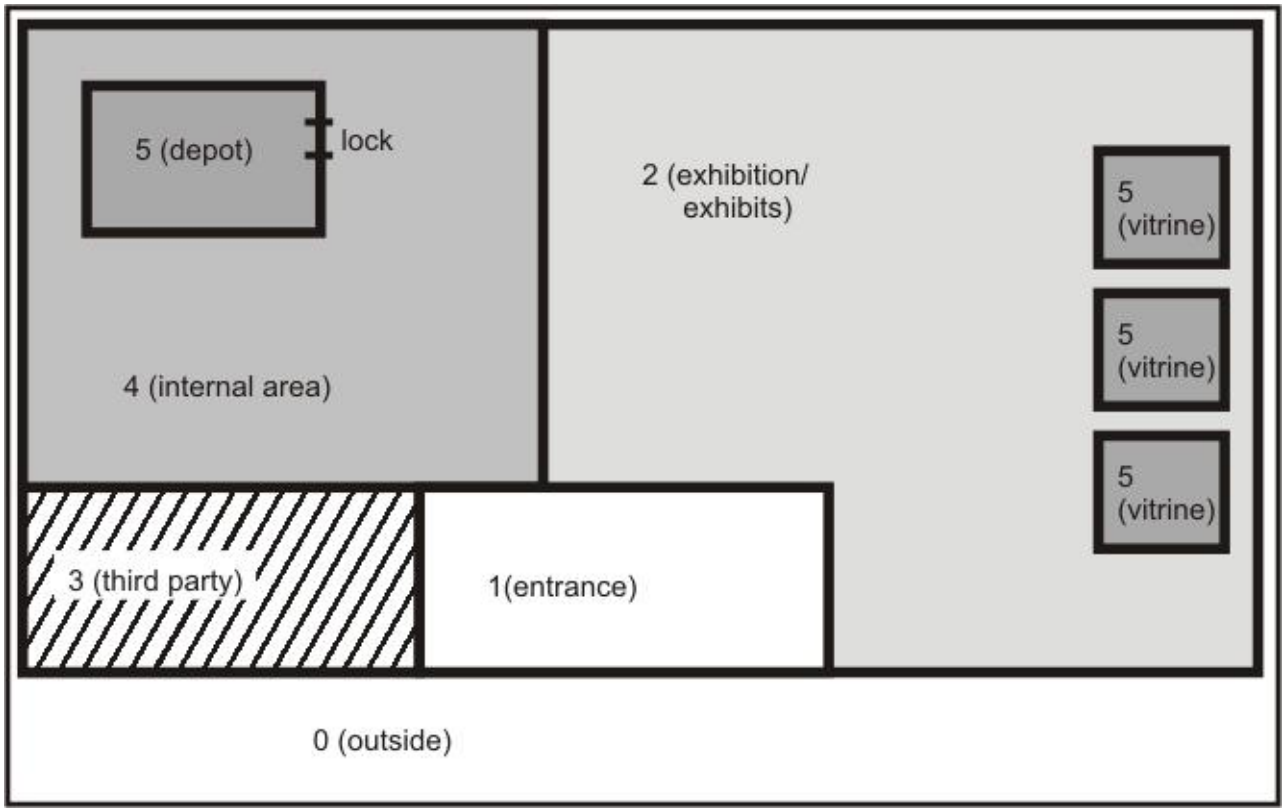

Figure 2-1 Sectors, schematic illustration

The risks should be assessed taking into consideration the different sectors of a museum (cf. Figure 2-1).

At the beginning of a risk analysis, the protection matrix below provides some first guidance. It illustrates the level and kind of protection required in different sectors.

Sector	Main risk	structural mechanical	IAS/HUAS[1)]	FDAS[2)]	VSS[3)]
0	Vandalism				
1	Burglary, vandalism				
2	Exposure, burglary, fire, vandalism, hold-up				
3	Burglary, fire, vandalism				
4	Burglary, fire, hold-up				
5	Burglary, fire, hold-up				

Table 2-1 Example or a protection matrix

There is a difference between buildings which are exclusively used as museums and those which are part of other organisations or whose premises can also be used entirely or partially by other organisations. While “pure“ exhibition centres can be locked after opening hours, buildings with shared occupancies always provide the possibility of entering outside opening hours. In any case, the museum’s rooms need to be partitioned from other – occupied – rooms. Any partition needs to accommodate mechanical safeguards, electronic surveillance and organisational protection measures. Such a shared occupancy may result from e.g. an integrated restaurant that is operated during and beyond opening hours.

In general, such risks may be posed by different groups of users such as employees, service providers or third parties without a traceable connection to the museum (e.g. visitors).

All the risks described below may result in immediate damage, for instance, stealing and destroying an exhibit. Moreover, almost every incident of immediate damage is expected to lead to indirect repercussions. For instance, if the best exhibit of an exhibition is stolen, the museum has to expect a decline in visitors or, worse, public interest drying up. If artefacts and collectors’ items are (perhaps repeatedly) stolen from a museum, this will have adverse effects on private and institutional collectors’ willingness to provide items on loan. If equipment that has been stolen or destroyed by e.g. fire smoke, this may paralyse or obstruct the museum’s operation for some time or bring it to a complete standstill. Other risks to the operation of a museum include natural hazards (storm, heavy rain etc.).

[1)] Intruder alarm system/Hold-up alarm system

[2)] Fire detection and alarm system

[3)] Video surveillance system

2.1 Burglary

Burglary crimes include burglary and theft and crimes such as

- Theft of objets d'art and collectors' items (or other desirable objects) during the opening hours of a museum
- "Smash and grab" theft
- Substitution of an exhibit by a replica
- Theft during shipment

All these crimes may also be committed by third parties who have no connection with the museum. At the same time, however,

- theft by museum employees
- theft by contractors' employees

also need to be taken into account when formulating the protection concept.

Burglary and theft (BT) as a particularly severe kind of theft is one of the most obvious risks to which objets d'art and cultural heritage are exposed. It has been estimated that global losses amount to several billion $US. Security experts need to tackle burglaries that may be aimed at exhibition halls as well as storage, utility rooms, external storage rooms or restoration workshops. Moreover, stolen objects of art and collections may be used to extort money (so-called artnapping).

The primary target of a burglary/theft is to steal objects of art or collections on display. Burglaries may also be aimed at other valuables such as admission money or change deposited in ticket booths or safety containers, IT equipment and office equipment.

Another risk, both to the structure of a museum and its exhibits and other fitments, may result from the successful entry of a perpetrator into the premises followed by wanton destruction as the individual searches for targets.

Theft by and/or following "sneak in" and/or "lock in" are special types of theft and are dealt with in the same way as burglaries. In these cases, the perpetrator hides in the museum or utility rooms which give him fairly easy access to the artefacts and collectors' items, making it possible for him to complete the crime after opening hours.

Crime preparations through e.g. manipulation or sabotage of security equipment in preparation for a subsequent attack also need to be taken into account for the protection concept. This implies attempted burglary by a perpetrator who opens or manipulates windows or doors during opening hours so that he can use them later, either for access or to escape.

The design of escape and evacuation routes can have a considerable impact on the risk of burglary.

2.2 Robbery hold-up

Robbery involving hold-up is a significant risk for museums. In a hold-up, the perpetrator threatens or exercises physical violence to achieve his goals. Threatening to use force helps the perpetrator to exert pressure to seize e.g. exhibits or cash (from admissions etc.).

Robbery crimes include the following acts by perpetrators:

- Robbery hold-ups during opening hours aimed at museum employees or visitors
- Intercepting museum employees when entering or leaving museum premises before or after opening hours
- Sneaking into premises during opening hours of the museum with the aim of a subsequent hold-up
- Breaking-in after opening hours with the aim of a subsequent robbery hold-up.

The risk of robbery hold-ups is particularly significant as it is not only directed at assets but it also, in particular, poses a risk to persons.

2.3 Vandalism

Vandalism in the broadest sense refers to deliberate, illegal damage or destruction of a third party's property; it is common in different forms. Vandalism directed at exhibits implies e.g. knocking over, breaking or spraying exhibits with the aim of partially or completely destroying them.

Vandalism is an offence to which there can be different underlying motivations:

- Malice
- Enjoying destruction
- Mental disorientation, emotional disorders
- Aggravation, bitterness, frustration
- Aversions against certain exhibition concepts and/or exhibits
- Destroying evidence, covering-up other crimes.

2.4 Fire and fire smoke

Fires (fire as well as smoke and heat) may have disastrous effects on people and exhibits, buildings and fitments.

The following factors pose the risk of fire development and spread:

- Arson
- Negligence (e.g. by unsuitable location for heaters)
- Defective (or obsolete) electrical systems and equipment
- Activities prone to cause fire (welding, soldering, hot-glueing, abrasive cutting etc.)
- Radiant heat by lights
- Handling flammable substances (including the risk of auto ignition)
- Open flames (candles, for example, during Advent in the foyer, at the ticket booth or in administration offices).

2.5 Natural hazards

Natural hazards include:

- Heavy rain and accumulation of waste water, e.g. due to technical problems in the sewerage system or the building's supply system
- Floods and storm surges
- Storm
- Hail
- Heavy snow
- Vibrations due to earthquakes, erosion, landslide.

2.6 Improper handling of artefacts and collectors' items

Risks as a result of improper handling of artefacts and collectors' items may be caused by museum employees in their daily routines, external service providers (e.g. cleaners, craftsmen) or visitors. Possible risks include:

Caused by museum staff:
e.g.

- Improper handling
- Improper storage
- Inadequate fastening (in an exhibition)
- Harmful environmental conditions in the exhibition damaging to exhibits (e.g. light, humidity, heat).

Caused by service providers:
e.g.
- Work carried out improperly (e.g. using wrong cleaning agents)
- Deviation from agreed procedures.

Caused by visitors:
e.g.
- Touching exhibits (touching, knocking over)
- Perspiration (causing humidity, carbon dioxyde).

2.7 Other hazards

In addition to the risks outlined above, the following hazards also need to be taken into account:

- Water pipes
- Sudden fluctuations in temperature and/or atmospheric humidity
- Humidity escaping from parts of the building (e.g. recent concrete construction).

3 Protection measures

Only well-coordinated overall prevention can achieve an adequate level of protection which makes the risk of loss, damage, destruction of valuables or obstruction to business calculable. When implementing the protection concept, administration, exhibition and storage sectors, security control room and perhaps workshops need to be distinguished.

Optimum protection of a museum can be achieved by taking into account different protection levels.

The entire outside area of the building needs to be included in the risk analysis. This also applies to the entire public area which is not necessarily the museum's responsibility and includes access roads, car parks etc.

The outer shell of the building, or perimeter needs to provide mechanical protection but also requires electronic surveillance. It makes sense to detect or report an intrusion at the moment that, or immediately after, the first mechanical barrier has been overcome. This should be followed by a second – stronger – mechanical barrier. In order to ensure effective intervention in the case of a burglary, the intruder alarm system (IAS) should be connected to an alarm receiving centre (ARC) or the police. The combination of mechanical and electronic safeguards achieves a high level of protection that also ensures an early activation of alarms.

Inside, an access control system (ACS) is able to monitor access to various sectors of the museum. ACS lent themselves to the control of those parts of the building to which only museum staff or a limited number of employees should have access.

Protecting selected exhibits poses a particular challenge. It is necessary to find customised solutions for particularly valuable objects. The selection of protection measures to be implemented needs to be agreed on a case-by-case basis.

Exhibits that require special protection (which may include originals as well as pieces that are exhibited as replica), in particular those that are not separately insured against theft, should be monitored around the clock by video surveillance system (VSS) – regardless of IAS surveillance.

It is necessary to ascertain whether there is an immediate risk to museum staff in addition to the risks to which exhibits are exposed. For instance, hold-up alarms could be installed in the foyer near the ticket booths which makes it possible for employees working in the ticket booth to call for help in case of danger. Using portable hold-up alarms should in some countries always be coordinated with the authorities, e.g. police, due to technical and organisational complexity, also in case they are connected to an alarm receiving and service centre (ARC).

Despite extensive technical safeguards, additional surveillance of assets by security personnel will be required during opening hours. Installation of VSS makes sense, although this does not necessarily

contribute to reducing the number of security guards required.

The protection concept should always be agreed with the insurer (in some countries with the authorities as well) and the planner of the exhibition at an early stage, which makes it possible to take into account expert know-ledge and loss experience in time. As the case may be, it helps to avoid necessary and costly security upgrades.

The protection and surveillance measures suitable for museums and showrooms are summarised and explained below. Mechanical safeguards should constitute the protection basis; they should be supplemented by electronic, organisational and personal surveillance measures.

3.1 Mechanical safeguards

Mechanical safeguards can be installed to protect the building on the one hand, and the collection's items on the other. Mechanical safeguards must not be neglected, even when buildings or objects are protected by electronic surveillance. Mechanical safeguards and electronic security technology complement one another. Replacing mechanical safeguards with intruder alarm technology is not acceptable judging by the experience of burglary insurers and the police.

Mechanical measures are the basic prerequisite for a viable protection concept as they effectively prevent potential perpetrators from easily entering the building and/or a protected area and gaining access to items from the museum's collection. Moreover, they make casual or opportunist theft more difficult.

An experienced security commissioner should be entrusted with the concept and maintenance of – both mechanical and electronic – security technology; he will also provide direct advice to the museum's management.

3.1.1 Walls

If walls are not sufficiently robust, a perpetrator can easily break through them. Attention must be paid to exhibition areas which are designed as individual protected zones; they need to have solid walls (as well as a solid ceiling and floor). It is possible that a perpetrator will try to enter through the ceiling (from the roof outside or through false ceilings inside) or through rooms on the lower floors.

There is a difference between walls of light construction without any special resistance to opening, walls of solid construction, e.g. concrete walls of 200 mm or more thickness. Walls of light construction are generally not suitable as outer walls (or as partitioning for rooms that house valuable artefacts and collectors' items).

Plaster, pugging and insulation do not enhance resistance.

3.1.2 Doors

Tested and approved burglar-resistant doors featuring at least class RC 2 according EN 1627 should be installed.

The main characteristics of a tested and approved burglar-resistant door shall include:

- Stable design of door leaf
- High-quality braces, possibly reinforced by lateral protection (in particular required for braces on the outside)
- Sophisticated locking system (in general multipoint locks)
- Burglar-resistant door plate
- Lock cylinder, protected against unlocking techniques, e.g. drilling and pulling, and resistant against picking and other manipulation methods
- Construction elements of potential weakness (e.g. glazed panels) are as solid as the entire door element
- Competent installation of the entire assembly (anchoring to the brickwork) in line with OEM specifications.

If no burglar-resistant doors are installed then (e.g.) additional locks and braces/lateral enforcements should be fitted to the existing doors to increase the protection level.

When upgrading a door or specifying a new one, it is vital to see to it that the old design and the new security elements are compatible.

The security upgrades must not obstruct escape and evacuation routes or render them ineffective. This must be taken into consideration during the planning stage.

Note: Doors in escape routes must generally open easily from inside and with a single push across the full width at any time.

Double doors/security gates

In most cases, doors in historical buildings need to be preserved and must not be changed. In these cases, a double door (burglar-resistant door behind the original door which cannot be protected at reasonable expense or for reasons/requirements of conservation of historical buildings) might be a possible solution provided the building's structure allows for its installation. This kind of protection is also suitable for other types of doors such as e.g. air locks to the storage, gates to underground car parks or escape staircases etc.

If someone tries to break in, an alarm triggered by the outer door would provide the optimum protection level. The inner door should serve as a burglar-resistant mechanical barrier. All solutions with intruder alarm systems need to see to it that "Safe setting" (see also chapter 3.2.6) is complied with.

3.1.3 Windows/Facade

Windows without burglar-resistant features can easily be overcome with simple tools in a matter of seconds.

This is why tested and approved burglar-resistant windows of at least class RC 2 (EN 1627) should be installed.

In terms of protection, domelights should be treated like windows. This also applies to glazed areas of the roof, (northlights, lantern lights etc.). When planning the safeguards, special attention must be paid to smoke and heat exhaust ventilation systems (SHEVs) or other ventilation openings. To some extent, these openings must comply with specified technical requirements while at the same time, be incorporated into the surveillance measures of the intruder alarm system.

The main features of a tested and approved burglar-resistant window include:

- Stable construction of leaf and frame of the window
- Attack resistant glazing
- Sophisticated fastening of glazing to leaf
- Wraparound burglar-resistant ironwork in combination with a lockable handle
- Competent installation of the entire assembly (anchoring in brickwork) in line with OEM specifications.

If burglar-resistant windows cannot be installed, the protection level of the windows needs to be enhanced by additional locks, for instance, or replacement of security furniture or, if possible, security glazing.

In general, historical windows cannot be secured. If such windows cannot be replaced for design or conservation reasons, the following safeguards might provide a solution:

- Iron bars
- Countersash windows (front window/second window)
- Inserting reinforced glazing (penetration for removal of objects and resistance to break-in).

Countersash windows

Countersash windows have a long tradition. In most cases, a single historical window can be supplemented by a second one. This is generally compliant with conservation requirements since the historical structure remains unchanged (see figures below). Figure 3-2 shows the original window and the added upgraded lock mechanics. The use of tested and certified furniture is recommended.

Figure 3-1 Countersash window, closed

From the point of security, climate control and conservation, countersash windows feature positive properties.

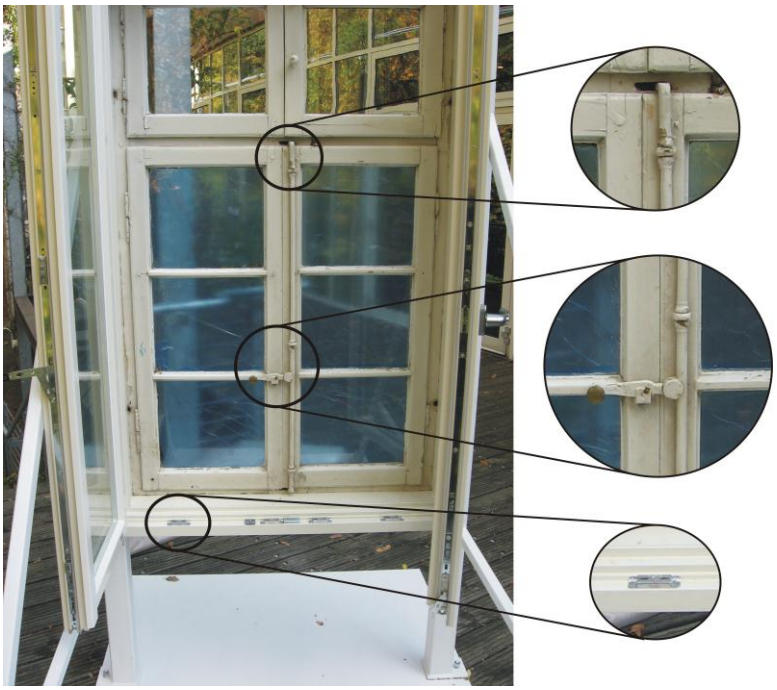

Figure 3-2 Contersash window, open

The outer window can be preserved to a large extent and/or re-stored from a conservation point of view. If need be, only intruder alarm sensors (contacts) need to be integrated into the outer window to monitor opening and closing. The outer window also needs to be sufficiently stable and robust in order to install an intruder alarm system that is almost 100 percent false-alarm-proof. It is necessary to decide on a case-by-case basis to what extent the window pane needs to be replaced by alarm glass (glass with integrated surveillance features) or whether another type of protection against penetration is required.

The inner window is designed in line with protection standards and features enhanced burglar-resistance. If possible, the inner window should be a tested burglar-resistant element.

If someone tries to break in, an alarm triggered by the outer window would provide the optimum protection level. The inner window should serve as a burglar-resistant mechanical barrier.

In individual cases, burglar-resistant blinds (installed inside) or shutters/lattice gates also provide a solution. A mechanically stable lining inside e.g. from plywood or sheet steel could also be a solution.

3.1.4 Other openings

Other openings that allow access (openings e.g. required for ventilation and air conditioning systems) also need to be secured by e.g. bars. Openings that are not used should be closed permanently by e.g. bricking up. The design drawings should be used to check whether previous openings have only been covered up with a thin plaster board for aesthetic reasons. Such covers hardly provide any mechanical resistance.

The maximum clear diameter of wall openings and spacing of bars should not exceed 12 cm and/or be reduced to that size. In general, openings with the following dimensions can be exploited:

- Rectangle of 400 x 250 mm
- Ellipse of 400 x 300 mm
- Circle of 350 mm diameter

In the case of openings needed for air circulation, it is necessary to bear in mind that bars reduce the free cross section and may effect air circulation. This must also be taken into account for pressure relief openings of gas extinguishing systems and of smoke and heat exhaust ventilation systems (see chapter 3.1.3)

3.1.5 Bars

Existing fixed bars may already feature burglar-resistant properties. In addition, tested and approved burglar-resistant bars may be installed.

Bars without certification need to comply with the following requirements:

- Steel
- Square bars having a minimum cross section of 16 x 16
- Round bars having a minimum cross section of 18 mm
- The bars are firmly anchored in the brickwork
- The size of openings between bars must not exceed 10 x 20 cm.

Bar to bar contact points should be fixed permanently, e.g. be welded together. In addition, the design requirements for burglar-resistant doors need to be taken into account when installing trellised gates. The following aspects also need to be considered:

- Bolt sockets of locks should be supported in the profile of the frame.
- The locking bolts should be protected against attacks by a continuous steel reinforcement in the frame.
- Penetration of and/or manipulation through the bars also need to be assumed. This could affect e.g. the fastening of the door's security fittings or even the door frame.

3.1.6 Roller shutter

Conventional roller shutters often do not have any burglar-resistant qualities. The installation of tested and approved roller shutters according, at least, to RC 2 (EN 1627) might be a solution for areas which have to be mechanically protected only outside opening hours.

Installing shutters on the inside of doors or windows might also be an option.

3.1.7 Mechanical protection

If the type of exhibit allows for it, mechanical safeguards should not be dispensed with, even when electronic surveillance is also used for the exhibit's protection. Quick removal of objects would at least be deterred in areas with public access. Figures, sculptures, paintings and other exposed exhibits should be effectively anchored in their positions.

Since in many cases, use of particularly mechanical safeguards, can mechanically damage an artefact or a collectors' item, they should only be deployed in close consultation with competent conservators.

It is necessary to consider whether the risk of the destruction of an object that is mechanically protected during its removal or attempted removal is greater than the risk of removal (intact) where protected only by electronic surveillance.

Mechanical safeguards and electronic surveillance should be harmonised in such a way that any forceful attack is electronically captured at an early stage and the mechanical component becomes operational afterwards.

3.1.7.1 Protecting freestanding items

Freestanding items should be secured at multiple points, if possible.

If possible, safeguards should not be detectable, and their fastenings should be concealed. However,

it is necessary to ensure that effective protection against dismantling of safeguards is still provided. In case of screw connections for instance, screws or lock mechanisms with a special mechanical code that can only be unscrewed with matching tools could be installed.

In individual cases, e.g. when an exhibit is in a wall recess, it might make sense to protect it with security glazing or bars.

Where many smaller objects need to be protected, a solution might be to partition the room, or at least part of the room, with glazing or bars.

3.1.7.2 Protecting paintings

Paintings should be secured in such a way that special tools have to be used to remove them. Hanging systems that protect paintings from quick removal and make it easier for museum operators to secure them have been proven to be effective. See example in Figure 3-3; a T-pin that is attached to the wall is inserted into a profile that can be mounted onto a picture frame. Adjustment options and a simple security device for hanging are also integrated.

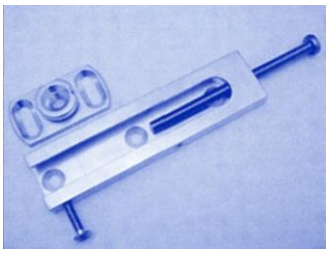

Figure 3-3 Hanging system

To protect valuable pictures and paintings from vandalism, they should be protected by special non-reflective front panels.

3.1.7.3 Security of display cases

Display cases are mainly used for safe presentation of exposed (small/valuable) exhibits.

Note: Aside from burglary protection, showcases may also provide protection against adverse environmental impacts (humidity, UV radiation, air-borne pollutants, temperature fluctuations etc.).

The optimum solution is a tested, burglar-resistant showcase. However, they are only provided by selected vendors, and it may not be possible to integrate them into every exhibition concept due to their design.

Experience shows that customised showcases need to meet the following requirements to confer minimum protection:

- Glass should be resistant to breaking
- Surfaces without glazing, e.g. cover, bottom, sides also need to have an attack resistant design
- The width of the frame design into which the glazing or any other filling can be inserted should be ca. 20 mm
- Weak points need to be secured against bending apart so that it is not possible to fish out small exhibits
- If possible, unframed showcases should be avoided.; Where they are nevertheless used, the glass panes should be glued together with high-strength glue (simple silicon gluing is not suitable)
- Locks (and bolts) need to feature the same burglar-resistant design to make it difficult to reach for the exhibits
- Locking cylinders should be secured against manipulation e.g. picking and feature protection against drilling and "pulling"
- Precautions are needed against dislodging and/or toppling over by screwing down to solid parts of the building
- Fixtures should only be accessible from inside. Alternatively, fixtures that are concealed or can only be dismantled with special tools can be installed
- In the case of valuable exhibits, electronic surveillance of the showcase should be considered (with the detector inside to detect opening, and reaching-in).

It has to be taken into account that even with fulfilment of these requirements, the showcase will

certainly not be comparable to the security level of a safe, but will only slow down the burglar. Thus additional security measures (perimeter etc.) may have to be applied.

Where visitors should have the ability to view particular exhibition rooms and/or areas which they cannot enter (e.g. living quarters with original furniture), glass partitions provide an option.

3.1.8 Safes

Valuable exhibits which are omitted from an exhibition or cannot be shown should be deposited in a special safe.

Safes and strongrooms are e.g. tested and approved in line with EN 1143-1, and classified in terms of resistance grades. Approved safes are labelled inside, e.g. VdS-approved safes are labelled inside with the blue approval badge shown in Figure 3-4.

Figure 3-4 Approval badge for safes

Safes, used in museums should be approved. Depending on the value of items to be deposited in the safe, suitable security features of the safe need to be agreed with the insurer in each individual case. Security experts generally recommend that the requirements for the deposit and storage of artefacts and collectors' items are agreed as early as possible with the insurer and the police in each individual case.

If the size and/or volume of the exhibits to be protected exceed the possibilities of conventional safe, a storage room should be considered as a separate protection zone. Aside from tested and certified strongrooms, storage might also be an option, depending on the local conditions. Their design should meet the following requirements:

- The construction of walls, ceiling and floor should be exceptionally strong
- Walls should not have windows
- Doors must at least meet class RC 2 (EN 1627)
- If ventilation openings are required, their clear width and/or height should not exceed 120 mm; if this is not possible, bars, if necessary with electronic surveillance, should be considered.
- Storage rooms must be subject to electronic surveillance (see chapter 3.2).

Aside from mechanical protection, security containers also provide a modest (but unspecified) fire resistance time. Fire and Thief resisting safes provide enhanced and defined fire protection.

3.2 Electronic surveillance

Intruder alarm systems (IAS) should be designed in such a way that intrusions/attempted intrusions are detected and notified as early as possible. In this context, mechanical safeguards and surveillance by an IAS, taking into account the expected intervention time, need to be harmonised in such a way that upon an alarm, intervention forces are able to arrive at the scene even before the perpetrator has managed to overcome the safeguards (see Figure 6.01). The interaction of electronic and mechanical safeguards needs to be fine-tuned to rule out the possibility of false alarms as far as possible.

In order to ensure the maximum level of functional reliability and monitoring effectiveness, installed intruder alarm systems should be certified. The intruder alarm systems that are suitable for museums feature different classes. In order to tailor the IAS to the risks at hand, classes are divided into e.g. class 3 or class 4 (EN 50136-1).

Intruder alarm systems of class 3 provide medium protection against attempted penetration in an activated and deactivated state (e.g. against sabotage). Intruder alarm systems of class 4 provide enhanced protection against penetration in an activated and deactivated state. Class 4 alarm systems also monitor safety-related functions.

Intruder alarms of class **3** are suitable for those areas of a museum that are less exposed, e.g. office and administration areas. To protect exhibition areas or individual exhibits, a class 4 IAS is generally suitable.

Depending on the type of exhibited and/or stored items, an IAS of class 3 to 4 might be suitable for exhibition areas and storage; for particularly valuable exhibits, a class 4 with additional special features might be required.

Certified IAS can be divided into several protected zones. The protected zones, in turn, may be attributed to different classes (e.g. storage meet class 4 and offices class 3). All system components of a protected zone need at least to meet the requirements of the respective class. Shared system components (e.g. intruder control and indicating equipment, transmission unit) need to comply with the highest class available.

Intruder alarm systems are able to accommodate other security features provided appropriate detectors are installed. The installation of hold-up alarms will convert an IAS to an intruder and hold-up alarm system; hold-up alarms are purely for the purpose of personal protection, and are permanently activated, regardless of whether the IAS itself is activated. Intruder alarm systems (IAS) and hold-up alarm systems (HUAS) may be combined with one another or designed as stand-alone systems.

Moreover, internal alarms and emergency calls, for instance, may be generated that notify a security control room and/or additional security personnel and/or activate a video surveillance system (VSS).

Note: Additional information can be found in national Guidelines for Planning and Installation of Intruder Alarm Systems.

Planning, installation and maintenance of a certified intruder and/or hold-up alarm system has to be carried out by a certified installer pursuant to national guidelines and documented in an as-fitted-document for the installation of the intruder alarm system. A certificate of installation of the IAS must be issued according to national requirements.

Intruder alarm technology, installers and security companies need to be tested and certified.

In the case of a connection to the police or an alarm receiving centre, the installer also has to fulfil national requirements. Intruder alarm systems may require the ability to generate a duress-alarm (hold-up alarm). In addition, control equipment with, for instance, a timer might be installed which only allows for IAS deactivation at specified and set times.

Aside from external activation, certain parts of the IAS can also be activated from inside. This makes it possible for instance, to monitor, in case of an alarm, certain rooms or contacts during the day without activating an external warning device or remote signal. This is a suitable option for all items monitored for removal and for doors in the course of escape and evacuation routes. Internal alarms may be forwarded to the in-house security control room or immediately notify museum or contractor security guards.

3.2.1 Surveillance concepts

Perimeter surveillance is intended to protect a building's perimeter (windows, doors, outer walls as well as ceilings and floors) from penetration. Openable elements such as e.g. windows and doors are also monitored for opening and closing. Perimeter surveillance has the advantage of being able to detect attacks on the building at an early stage. The combination of perimeter surveillance with a well-aligned mechanical barrier in the perimeter is able to achieve a high level of protection, which provides for security and, at the same time, gives intervention forces the opportunity to catch a perpetrator in the act of crime.

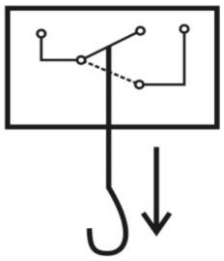

Figure 3-5 Detector of a painting, schematic illustration

The purpose of **focal point surveillance** is to detect a perpetrator who has already entered a building (through, e.g. motion detectors). In this case, the surveillance of every room is not necessary. Focal point surveillance can also combine electronic surveillance with mechanical safeguards, so that a perpetrator who triggered an alarm is obstructed or held back by additional mechanical barriers; this increases the chance of catching the perpetrator in the act.

The negative aspect of focal point surveillance as opposed to perimeter surveillance is that the perpetrator can only be detected after entering the building. Focal point surveillance may be installed to complement perimeter surveillance in order to detect perpetrators who e.g. sneaked in.

Trap protection is used to monitor with an IAS only certain parts which the perpetrator will most likely enter, e.g. a vestibule that the perpetrator crosses to enter other rooms (so-called traffic routes). As with focal point surveillance, the drawback of trap protection vs. perimeter surveillance is that the perpetrator (sneak-in perpetrator) can only be detected once he is already inside the building.

Object surveillance refers to the targeted monitoring of certain objects, e.g. sculptures, paintings, showcases or security containers.

3.2.2 Special detectors

Several surveillance measures for different types of risk exist. These highly specific solutions may be required for electronic surveillance of objects of art and culture in detail. Some of these specific solutions will be described in the next paragraphs.

Electromechanical and/or electronic detector of a painting

These detectors monitor whether a painting is still in its place, using e.g. an electric contact that is kept closed by the weight of the framed painting (see schematic illustration in Figure 3-5). If the force by which the contact is activated changes too much (e.g. by taking the painting off), the contact opens and an alarm is triggered.

Detector to monitor the canvas

Special detectors can be used to monitor the canvas of paintings. If someone tries to remove the whole painting or its canvas, an alarm is triggered. A mechanical switch (see Figure 3-6) or optical system monitors the position of the canvas. For the optical system, the back of the canvas has to be illuminated with (low-energy localised) lights. Changes in light reflection are captured and used as a detection criterion.

Figure 3-6 Canvas detector

Detectors that operate capacitively

These detectors form an electric field around the object. Changes in this field which are created e.g. by a person approaching the object (through the field) are captured as detection criteria. The principle of capacitive surveillance can be applied to a multitude of artefacts, such as stand-alone objects, showcases (entirely or its contents only), paintings etc. Objects to be protected by capacitive surveillance might need to be prepared, e.g. by applying a conductive film onto the back or bottom of the exhibit.

Tear-off detector

Tear-off detectors can be used to protect objects that are fixed to their spot. If the object is removed,

an alarm is triggered. Tear-off detectors can be installed e.g. by special screws (monitoring a pre-determined breaking point and, if necessary, activating an alarm).

Combination detector

Different types of detector can be combined in one product. For instance, different types of motion detectors or motion detectors with the option of video recording and alarm image storage can be combined with one another. The special logical connection of the functional principles makes it possible to relax certain application restrictions (e.g. no installation close to ventilation systems) listed in national guidelines for planning and installation depending on the detection principle. National regulations may require that only approved detector settings in line with the technical documentation of the system's certificate holder are used.

3.2.3 Hold-up detector

Hold-up detectors should be predominantly installed in high-risk areas (e.g. near the ticket office) or areas which allow observation of high-risk areas. Hold-up detectors should also be installed in any room in which a person could be imprisoned by a perpetrator. Hold-up detectors must not be easily identifiable to third parties. They need to be installed in such a way that the perpetrator will not notice activation of the detector or an activation signal attached to the detector. The detectors should be positioned in such a way that spurious activation of an alarm is avoided. Installation of radio hold-up detectors should be considered taking into account the risk level.

If intruder alarm systems are equipped with hold-up detectors or if separate hold-up alarm systems are installed, a fundamental difference between the hold-up alarm system (HUAS) and the intruder alarm system has to be taken into account. In the event of acute danger, the HUAS is used to trigger a remote alarm manually. To trigger a hold-up alarm, a targeted manual operation (wilful activation of a hold-up detector) has to be performed.

Activation of a hold-up alarm is possible at any time, including in its externally deactivated state, e.g. during normal business hours.

*Note: Due to unpredictable responses by perpetrators, hold-up alarms should never be allowed to trigger an external alarm or an internal alarm (i.e. no activation of any type of warning device*s*).*

3.2.4 Protected zones

Protected zones are separate rooms and sectors of the area monitored by the IAS. They may be defined individually within a building. Individual plans can be developed and protected zones designated for rooms that require a high protection level but are not constantly frequented (e.g. storage); their systems can be separately activated/deactivated. The protection systems of these zones should generally be activated. They should only be deactivated when authorised personnel enter them.

Due to organisational demands, e.g. rooms being used by third parties, entering of contractors (e.g. cleaning staff), different working hours of museum employees, necessary maintenance work or multiple occupancies of rooms, it might be necessary to adapt the division of protected zones to individual circumstances. More specific information on the requirements and options of protecting a building by an IAS can be obtained from national guidelines.

It is possible to install

- separated
- dependent and
- independent protected zones.

Separated protected zones are separated from the (actual) protected zone. Activation/deactivation of both sectors is simultaneous.

Dependent protected zones are activated or deactivated consecutively in a specified sequence.

Independent protected zones do not influence one another. They can be individually activated or deactivated.

When planning the protected zones, it is necessary to take into account the direction of escape routes. Escape doors must not lead into a room protected by an IAS.

3.2.5 Intruder control and indicating equipment

Intruder control and indicating equipment – the IAS' brain – should be installed in the monitoring range of an intruder detector and a place which is not generally accessible. It needs to be installed in such a way that it or any displayed indications cannot be observed by unauthorised people within or outside the protected zone, and such that unhindered access to it is prevented. It might be desirable to have a display of the IAS' status - regardless of the location of the intruder control and indicating equipment – e.g. in the security control room (it is necessary to ensure that the control room is accessible to authorised personnel only).

In the case of intruder control and indicating equipment featuring hold-up detectors, it is necessary to ensure that the perpetrator is not made aware of the activation of a hold-up alarm (e.g. inconspicuous signals, no acoustic signal).

In those cases where a shock criminal attack on these components is possible, they require mechanical protection in addition (e.g. a robust steel cabinet that can be locked).

If several protected zones are protected by an IAS, the intruder control and indicating equipment needs to be installed in the protected zone that is activated first and deactivated last. If required, a separate protected zone has to be installed for the intruder control and indicating equipment.

3.2.6 Safe setting

Compliance with so called Safe setting for intruder alarm systems approved by the authorities is mandatory in some countries and provides the maximum level of reliability and comfort for the operator that the IAS is properly activated and deactivated. Safe setting means the following:

Note: Safe setting assures by technical means that an intruder alarm system on the one hand can only be put into the set-condition ("ready for alarm") if all surveilled windows and doors are closed and properly locked; on the other hand it is assured that an IAS-surveilled room, house or flat can only be acceded after the IAS was put into the unset-condition (the IAS was "switched of"). By this false alarms are being avoided which sustain the authenticity of the system.

- Prevents the operator from accidentally entering areas of the IAS where the protection is set (in operation) through technical and structural barriers
  (the protected area cannot be accessed without prior deactivation as the last barrier is unlocked immediately upon deactivation).
- Ensures that all monitored doors and windows are properly closed and all detectors are non-operative prior to external deactivation
  (closing of windows and access gates is electronically monitored, the control equipment is not operational when windows and access gates are not closed).

3.2.7 Types of IAS alarms

There are three different types of alarm activation which are often used in combination

- Internal alarm
- External alarm
- Remote alarm.

Internal alarm is activated inside the IAS' range. In general, an acoustic warning device is used for internal alarm activation, while optical warning devices are an option. Depending on the IAS concept, an internally activated IAS may trigger certain detectors (e.g. private doors, picture detector) that notify the in-house security control room and/or external security personnel. In-house security guards can also be notified immediately by radio transmitters or receivers (often referred to as pagers).

External alarms make use of optical and/or acoustic warning devices (flashing light, siren) to notify the general public. The warning device, in particular the siren, also makes it obvious to the perpetrator

that the intrusion has been detected. External warning devices may also be installed within the monitoring range in order to directly deter the perpetrator/s.

It is not certain, however, to what extent the general public respond to the optical or acoustic signals and respond by notifying (e.g.) the police.

- Property insurers and the police do not recommend use of external alarms alone.

In general, a **remote alarm** is transmitted via a phone or data transmission line (e.g. telephone or internet). Its purpose is to notify a central organisational unit (e.g. security company, police) of an intrusion. The risk of a sabotage attack on the transmission path can be prevented by installing a certified IAS, using certified and secured transmission paths and equipment.

- Class 3 and 4 IAS requires activation of external alarm in addition to remote alarm. The desired deterrent effect on perpetrators can be achieved by external acoustic warning devices in the protected zone.
- When the system is directly connected to the police, installation of the external alarm has to be agreed with the police according to national requirements.

3.2.8 Intervention

Alarms by an intruder alarm system can only be effective if they lead to suitable intervention measures.

When intervention measures are agreed, it is necessary to specify whether the keys for the premises are deposited with museum staff or an intervention centre. In case the IAS triggers an alarm, the key must be available on site at short notice. In order to ensure a swift and effective operation of the intervention team in the case of an alarm, intervention plans need to be formulated in advance.

The operator of the IAS, the security company and, if necessary, the police should agree suitable corrective actions prioritised in line with their importance, to respond to different potential alarms, they should documented in the certificate for alarm and intervention services. In the case of premises protected by an alarm, the security company (ARC) may swiftly carry out the agreed measures one by one, ensuring the maximum success of the intervention. It is vital to regularly check all data recorded in the intervention measures to see whether they are still up to date since telephone numbers and names of contacts etc. may change.

See also chapter 3.4 Video technology.

3.3 Access control

The installation of a certified access control system (ACS) is a viable option for rooms that are accessible to authorised personnel only. Information on how to plan and install ACS is contained in national guidelines. ACS may also be installed separately from intruder alarm systems, e.g. in areas that are not monitored, or during normal business when the IAS is deactivated. Access to rooms that require a higher security level should generally be managed by an ACS. These include the store, server and IT rooms, restoration workshops etc.

If there is a need for enhanced security, motor-operated locks and/or self-locking electromechanical locks should be installed rather than electrical door openers only.

The ACS needs to be set in such a way that access authorisation and keys issued (including keycards or mnemonic codes such as combinations of number or letters) are assigned to certain persons. This makes it possible to identify and record when someone enters or leaves a room, which key he/she is using and who is the “owner” of that key.

Biometric systems may be a feasible option for areas that are particularly exposed. However, before installation of such a system, it is necessary to ascertain whether the false acceptance rate (FAR) and/or the false reject rate (FRR) of the biometric system are acceptable for the respective application. Biometric systems can be combined with conventional transponder systems, which may prolong the processing time of an actuation.

Organisations that are extremely exposed may require additional measures such as security checks of individuals, isolation, checks for weapons (metal detectors) or other precautions.

3.4 Video technology

Video technology makes it possible to capture, and report criminal events and record their course. More sophisticated technologies make it possible to detect and identify perpetrators. When installing video technology, it is necessary to make sure that data protection provisions, employees' rights etc. are not violated.

Pursuant to national regulations, a sign (see e.g. Figure 3-7) has to indicate to the public that video surveillance is in place. The organisation responsible for recording (e.g. name of the museum where the video recording is made) should be indicated below the sign.

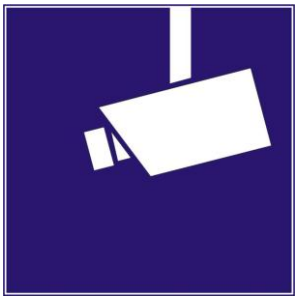

Figure 3-7 Indication of video surveillance

3.4.1 Purpose of video technology

The purpose of video surveillance systems (VSS) is to extend the possibilities of optical surveillance; they enable security personnel to monitor not only their immediate environment but also rooms and objects that are far away. Moreover, if required, focal points may be designated for surveillance.

Where there is a discrepancy or a suspicious situation, immediate notification of the security guards on site, e.g. by radio communication, mobile phone or pager, has to be ensured to be able to take action immediately.

Note: There is a danger in assuming that the functions of security personnel can be completely and satisfactorily replicated by video technology.

3.4.2 Applications

If cameras are positioned in such a way that all relevant areas are visible, security personnel are able to reduce the number of patrol 'rounds' depending on the risk situation, or use the cameras to pre-select and view the areas that will be covered during the round.

Monitoring of escape routes

VSS are viable options for monitoring escape routes for the purpose of both personal protection (e.g. to check whether escape routes can be used safely in case of a fire) and asset protection (e.g. to check whether a perpetrator attempts to use escape routes to escape).

Deterrence

The deterring effect on potential perpetrators is similar to that of lighting systems (cf. chapter 5.1.). There is no evidence of the deterring effect, – as it is not evident what effect a visual inspection and/or recording has for a perpetrator – but the effect can be reliably assumed.

Preliminary alarm checks

IAS with In the event of an alarm activation, the security personnel can carry out a quick and effective preliminary check. If the security guards are familiar with their environment, the exhibits, and the respective surveillance range of the cameras, and if they are trained regularly, they are competent to do so.

The extent to which preliminary alarm checks by a VSS make sense in the event that a remote alarm is triggered by a security company needs to be determined on a case-by-case basis. It is in particular essential to determine who is responsible for deciding whether to intervene or not to intervene, and which criteria form the basis to decide whether or not to take action.

In general, a remote alarm should not be ignored simply on the grounds that the video image does not show any indications of an intrusion. Usually, although the video images transmitted may indicate that there is no immediate danger, an intervention can be carried out with minimum resources.

Should a burglary be detected by the video technology, the police can be notified immediately, which saves valuable time otherwise required for preliminary alarm checks (cf. Figure 3-8). The odds of catching a perpetrator in the act of crime, and thus prevent loss of exhibits, improve the less time is used for preliminary alarm checks (response to alarm activation) and the faster the actual intervention (attempts at catching the perpetrator) can be launched.

Evaluating progression of events

State-of-the-art video surveillance systems (VSS) save *all* images recorded for a certain period of time. Their magnetic core memory makes it possible to view and evaluate events prior to, during and after the actual crime. If required, the findings can be used for investigation purposes or the planning of counter action.

Information for manhunt and conservation of evidence

If the recording quality is adequate, video material can provide useful information for the police investigation after a theft or any other damage. Video technology, designed and installed pursuant to national guidelines meets these strict requirements.

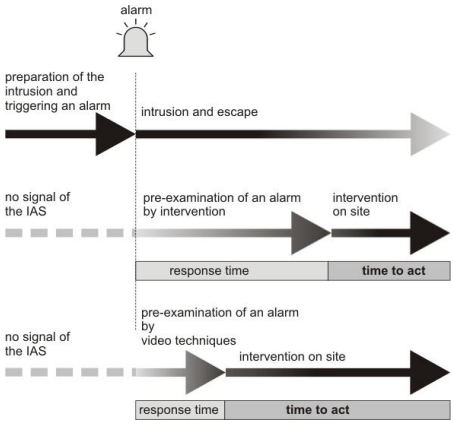

Figure 3-8 Preliminary alarm check

Video sensor technology

VSS may feature special video sensors that detect motion and signal an alert.

Surveillance of removal

Modern VSS systems process changes of an image that happen without any detectable motion in the scene. These cameras detect removal of a painting even if the camera view is restricted to a certain angle.

Add-on to ACS

Video technology can be added to the access control system. With VSS in the entrance area, it may be possible e.g. to grant access to certain persons who need not produce evidence of identification to the ACS. Moreover, even with an ACS, the VSS may have an additional control function if the immediate entrance area (either permanently or during a security round) is within a security guard's view. The security guard does not necessarily have to be posted at the door.

Outdoor application

In order to optimise outdoor application of VSS, movable objects up to a certain size may be filtered out. Thus, small animals moving within the camera range can be tolerated. Other restrictions on the use of video technology in public areas need to be complied with.

3.4.3 Camera location

Complementing access control systems by video surveillance systems (mounting cameras at access doors) is a feasible option as much as surveillance of individual objects or areas that are particularly exposed.

As a minimum all emergency exits leading from the building to public premises should be monitored by video cameras. Even though this may not prevent theft, the cameras are able to spot a thief who is trying to get away with his loot through the emergency exit, and interventions can be initiated immediately.

Note: Doors in escape routes must generally open easily from inside and with a single push across the full width at any time.

3.4.4 Documentation

The video surveillance system installed has to be documented in a special certificate. The certificate for a video surveillance system should include all important data on the system such as which system components have been used and where they have been installed relative to the object.

The installation certificate makes it possible to obtain a reliable overview of the VSS in order to

develop further measures in the context, for instance, of a protection plan.

In addition, the installation certificate provides certainty to installers and operators. It documents exactly what the installer agreed and subsequently realised at the request of the operator. Special solutions or permitted deviations from requirements defined by planning guidelines are also explained and documented by the certificate. Failure to take certain action, e.g. no camera surveillance at exits, must also be documented to be able to track decisions and agreements.

3.5 Protection against vandalism

Various mechanical safeguards, in particular surveillance by security guards, may be used as targeted protection against vandalism.

Technical precautions against vandalism make it more difficult for a perpetrator to access the object to be protected. They may include:

- Transparent panes in front of the object
- Storage/exhibition of items in showcases
- If possible, exhibition of realistic copies.

Surveillance by security personnel is designed to influence visitors' behaviour in such a way that they cannot damage objects in any way. Upon entering the premises, security guards urge visitors to deposit large bags, backpacks, umbrellas etc. at the reception or cloakroom so that potentially damaging objects cannot enter exhibition areas. In the exhibition area the security guards shall be ready to react on suspicious behaviour and take appropriate action.

As vandalism occurs rather during normal opening hours than following a burglary, it is of paramount importance to raise the awareness of, and properly train, security personnel.

3.6 Fire protection

The risk of fire (fire, heat, smoke and fire gases, extinguishing water etc.) in museums and other facilities that exhibit objects of art and cultural heritage poses a serious threat to these organisations. Although a fire and loss of profits insurance policy may compensate for the material damage caused by a fire, the personal injuries and the damage resulting from partial or total loss of artefacts and collectors' items which are irreplaceable are much more serious.

The damage that such a negative incident can do to a museum's image must not be underestimated either. Preventive fire protection measures are able to mitigate the fire risk in museums and showrooms effectively. Intelligent investments in structural and technical features in combination with organisational measures ensure safe operation of museums and showrooms.

This not only applies to new buildings; suitable measures are capable of realising improvements in old buildings. Pursuant to the relevant legal standards of the Federal States (regional building codes, industrial health and safety laws), the operator is obliged to determine and implement the necessary precautions.

Effective fire protection can only be achieved by a holistic fire protection concept tailored to the respective museum. This brings all individual protection measures into line. A fire protection concept includes measures of preventive fire protection (with individual structural, system-related and operational/organisational elements) as well as fire defence that consist of rescue and fire-fighting operations. All these necessary components interact with each other. For more information and guidance reference is made to the CFPA-E-guidelines "Fire Safety in Museums of Paintings".

3.7 Water and other natural and environmental hazards

In addition to the risks of fire, burglary/theft, robbery and vandalism outlined above, works of art and collectors' items of special value also need to be protected against a range of other hazards since these supposed minor and often underestimated hazards have a great potential for damage and destruction.

3.7.1 Damage caused by water

Damage caused by water may have manifold causes. Aside from damaged water pipes (water escaping from feeding and discharge pipes of the water supply), this category also includes damage caused by heavy rain, back pressure due to weather conditions or extinguishing water.

In general, museums and all their supply and discharge systems, exhibition and storage rooms, need to be designed in such a way that they are protected against water penetration. If possible, storage rooms should have pipes which are not permanently water-bearing.

Museums and showrooms should not be situated in

- Areas exposed to flooding and

Areas with works of art that require special protection should not be accommodated

- Directly underneath flat roof areas with expansion joints and inlets
- Underneath water tanks.

If these risks cannot be avoided, protective measures suitable for the respective situation must be taken. These may include:

- Storage of artefacts and collectors' items above ground level (elevated racks, shelve storage) - the minimum height should be 12 cm (Euro palette)
- Avoiding plug-in connections (power supply and data cables) in false floors or directly in floors; should it not be possible to avoid plug-in connections they should have IP 54 safety design
- Water dams
- Anti-flooding flaps in the waste water and rainwater pipes (special attention on regular maintenance and inspection)
- Water detectors connected to the alarm system
- Pump well with automatic lifting pump
- Collection tanks under potential weak spots connected to the building's drainage system (e.g. below the cooling aggregates of air-conditioning systems in the storage)
- Pipes (e.g. for waste water, steam, fresh water supply, heating) – even those in suspended ceilings – should be removed, if possible.

Further information can be taken from CFPA Europe 1-2012/N Protection against flood.

Should it not be possible to avoid water-bearing pipes for technical reasons, the following precautions must be taken:

- The material of the pipes must be anti-corrosive and suitable to withstand the specified pressure. Suitable methods must be applied to check welded joints for cracks.
- The pipes should be double-walled (either directly or by subsequent encasing). Humidity sensors should be installed in the outer shell; their signals transmitted to a contingency organisation manned 24/7.
- The water pipes monitored by humidity sensors need to be isolated by electrical valves (that can be closed without power) installed outside the risk area.
- Check valves should be easily accessible and clearly labelled.

3.7.2 Damage caused by natural hazards

In addition to the risk outlined in chapter 3.7, other conceivable natural hazards such as earthquakes, landslide, the weight of snow and avalanches need to be taken into consideration, in particular during the planning phase. As these hazard depend to a large extent on the position (e.g. on a hill or slope) of the respective museum and/or showroom, customised concepts need to be developed for natural hazards.

An appropriate design of the building structure can prevent, or at least significantly reduce, any damage caused by natural hazards. This applies in particular to damage caused by erosion, strong wind or hail. Moreover, support structures and/or deflector barriers provide effective loss prevention against heavy snow and/or avalanches.

3.7.3 Damage caused by lightning strike and overvoltage

Damage by indirect, and particularly direct strike, of lightning may be reduced significantly by suitable protection concepts. A competent specialist planner, e.g. a certified EMC expert is able to develop a comprehensive concept for overvoltage protection.

Electromagnetic fields emitted e.g. by mobile phones or other radio transmitters can cause interference, and suitable counter measures need to be specified (e.g. banning mobile phones).

3.8 Documentation

Documentation of all technical measures (air conditioning systems and their configuration, fire protection, security and access control systems etc.) constitutes the basis for a smooth operation as well as effective trouble-shooting. It must be updated continuously.

The following elements (this list does not claim to be complete or inclusive) should be part of the documentation:

- Structural plans
  - Site map (premises)
  - All architectural and detailed design plans
  - Ground plan/floor plan/occupancy plan
  - Plan of water-bearing systems in/above risk-relevant areas
  - Water retention concept
- Electrical drawings for
  - Energy supply
  - certified Lightning/ overvoltage protection
  - Potential equalizer
  - Flow diagrams
- Fire protection concept
  - Fire protection plan (alarm and fire brigade operations plan)
  - Fire safety regulations
- Security technology
  - Intruder alarm system (IAS)
  - Fire detection and alarm system (FDAS)
  - Access control system (ACS)
  - Video surveillance system (VSS)
- Contingency planning
  - Emergency telephone list
  - Supplier list
  - Plans to take exhibits out of storage.

All systems and installations available, as well as all implemented loss prevention measures, must be documented. Information has to be added or changed in the documentation whenever extensions are made or refurbishments carried out.

Such documentation should be compiled during the planning stage of a museum (or, if necessary, individual exhibitions).

3.9 Handling and treatment of artefacts and collectors' items

Artefacts and collectors' items should only be handled and treated by competent and specially qualified staff. In order to ensure proper and appropriate handling of every object, an internal quality management system should describe all relevant activities by way of procedures, specifications and standards for documenting all relevant tasks.

Damage by visitors or other third parties can only be avoided if people are kept away from the respective exhibit or by effective supervision.

Adequate protection of an exhibit against accidental damage by visitors can be achieved by providing "virtual" barriers for objects of minor value, e.g. by cordoning off an exhibit. It helps to prevent accidental contact.

3.10 Technical installations

3.10.1 Electrical installation

Electrical installations are to be installed and maintained in line with approved electrical engineering standards. The Installation network of new systems need to be designed as a TN-S system throughout the building in line with the series of standards HD 60364 (Low-voltage electrical installations – Part 4-41: Protection for safety – Protection against electric shock (IEC 60364-4-41:2005, modified)). The most important benefits of a TN-S system include:

- an isolated neutral conductor throughout the entire building
- protection and potential equalizer to a large extent free of operating current
- predominantly avoiding adverse stray current in conducting parts of the building and piping.

In order to ensure these prerequisites on a continued basis, permanent monitoring of fault current should be installed that triggers an alarm when the limit is exceeded, notifying the relevant people.

In order to enhance a fail-safe operation, it is possible to install redundancies of important cables and power lines, regardless of the protection required.

To enhance technical safety, certified lights should be installed. HD 60364 and further national requirements shall be considered for installation of lighting systems.

Note: Conventional low-voltage halogen lights develop a high temperature at close range. This may result in discolouration of surfaces or more profound direct surface damage and even cause a fire.

Moreover, safe data transmission and safe internal and external communication must be ensured.

3.10.2 Air conditioning/ventilation systems

The prerequisite for proper climate control of all rooms is compliance with limits for ambient temperature and humidity defined by the art experts of the respective museum.

A monitoring system that is isolated from the air conditioning and ventilation system should be installed; it monitors the air conditioning system to maintain specified limits for temperature and humidity; if these limits are exceeded, the monitoring system triggers a signal and/or shuts-down the air conditioning. The signals should be transmitted to a control room that is manned permanently.

3.11 Security fog devices

A security fog device (sometimes referred to as a ‘smoke’ security device) is a security system which, on activation, produces dense fog in order to disorientate a potential thief or aggressor and thereby deter/hinder further access into the protected area and/or disrupt a hold-up in this way.

When a security fog device activates, the ‘fog’ is produced extremely rapidly and the protected area will be filled in a matter of seconds, completely obscuring vision. Dispersion will occur either naturally over a period of time or more rapidly with venting via opened (or broken) doors and windows.

Security fog devices were originally designed primarily to combat ‘break-in and grab’ style theft, where more conventional security devices failed to prevent or deter losses.

They also are also used to provide useful protection during the time interval between an intruder alarm activating following a break in, and the arrival at the premises of a human response, from security guard, keyholders and police, for example.

Increasingly, security fog systems are being been used by e.g. banks and jewellers as a defence against day-time raids. Hold up device activated anti-raid security fog systems are designed to ‘push’ the attackers away from the staff area towards the outside. Typically, the fog deployment will be accompanied by an automated, pre-recorded verbal warning intended to reassure lawful customers that a security system has been activated, that the fog is harmless and that the police have been called and will arrive shortly.

These systems are clearly a radical solution (often seen as a “last resort”) which can be introduced into any workplace or publicly accessible area only after a very careful assessment and that the safety and security of staff and customers will be enhanced, not jeopardised, by its deployment.

In particular:

- the museum must be totally satisfied that the fog will not have any adverse effects on sensitive objects such as paintings
- the police will not enter a fog-filled environment but will wait until the fog has dissipated
- all persons (including customers and staff) leaving such area are potentially liable to be treated as potentially dangerous suspects by any responding police officers waiting outside
- all staff must be fully trained in the correct use of the system and witness a test or demonstration discharge
- if used as a hold-up solution is important to be satisfied that any installation proposed will perform sufficiently rapidly and effectively to meet this specific operational requirement.

Note: This solution is controversial and is not necessarily permitted by insurers or national authorities such as regulatory bodies, police etc.

4 Organisation

Aside from the mechanical safeguards and electronic measures (e.g. intruder alarm system and video technology, access control), organisational measures constitute the third element of the security system.

Organisational measures include instructing personnel on potentially dangerous situations, administering keys and allocating access authorisation, drawing up an inventory of objects of art and cultural heritage available and developing evacuation and salvage plans for objects of art and culture (*Note:* a CFPA guideline is under development). Moreover, clear procedures for operation of mechanical safeguards and electronic surveillance measures need to be defined. The best security system is useless if it is not properly operated and/or activated.

Small exhibits that are difficult to protect by mechanical safeguards should be as far away from escape doors as possible.

4.1 Security commissioner

In order to implement security policies, it makes sense to appoint a certified security commissioner as the individual responsible for security. He/she should report directly to the museum's management/management board. The security commissioner assesses all risks associated with asset protection and develops appropriate counter measures. The risk and security analysis of the security commissioner makes it possible for the museum's management/management board to take all relevant decisions.

4.2 Security regulations

Due to their importance, security regulations need to be put into force by the museum's management/management board and communicated to all employees. The security regulations need to be constantly kept up to date, taking in particular into account changes in procedures and structural systems. They must contain the most important measures of asset protection and specify how to behave during and after a theft, a vandalism attack or any other attack on the museum's assets.

The following list provides some first guidance; however, it needs to be adapted to the respective risk:

- Establish the values available
- Estimate to what extent these values will attract perpetrators
- Identify specific risks (e.g. the possibility of an item being damaged or stolen)
- Develop optimum protection measures
- Determine affordable security measures
- Define how to behave during and/or after a loss
- Coordinate measures to be implemented with museum's management/management board
- Museum's management/management board puts security regulations into force.

4.3 Security control room, internal

The in-house security control room – also referred to as the 24/7 control room– operated during opening hours of the museum and/or round the clock, is qualified to coordinate protection measures and effective intervention measures. All information relevant to the museum's security must be pooled by this control room. In-house procedures are then applied to process this information one-by-one.

The necessary technical systems and equipment to this end must be provided. Operating panels and information displays of the intruder alarm system and monitors for the potential video surveillance system must be installed. Appropriate means of communication with the supervising staff must be provided.

When the security control room is built for the supervising staff working there, structural protection against possible threats from outside must be provided.

4.4 Supervision

To monitor visitors' behaviour in exhibition halls, security guards should be deployed. They should be easily identifiable by uniforms or other characteristics to stand out from the visitors.

The security guards, museum staff or employees of service providers, need to be trained on a regular basis and briefed about the exhibition and its importance. They need to be familiar with their legal rights in relation to visitors. Depending on the type of exhibition, the number of security guards needs to be determined on a case-by-case basis. The area to be monitored must not be too large and/or muddled; and the value of exhibits and their removability must be taken into account.

Cleaning staff and other staff present, craftsmen etc. need to be supervised when they work beyond opening hours. An adequate number of security guards should also be present during any set-up or dismantling jobs.

Before the security system of an exhibition's protected zone is activated, the exhibits need to be checked to make sure that they are intact and all in their place, locks of doors and showcases must be inspected to make sure they are in operation and show no traces of manipulation. The rooms need to be screened to make sure that there is no one inside, while areas such as blind spots (potential hiding spots) need to double-checked. Removal of objects e.g. by restorers needs to be reported and/or indicated to the security personnel.

4.5 Cloakroom

Visitors should not be able to enter the exhibition with coats and other large items of clothing, bags, purses, backpacks etc. not only for reasons of burglary protection but also for reasons of conservation. For this purpose, enough cloakrooms and/or lockers must be provided. If the cloakroom and/or lockers is/are full, additional visitors should be denied access for as long as there is no room to deposit coats/bags.

In the case of special events with a large number of visitors, additional cloakrooms must be provided, e.g. by using neighbouring rooms for this purpose.

4.6 Keys and key authorisation

Whenever a key is issued, this must be logged, which can be done manually in a keys' log or a so-called key management and/or transfer system. Access authorisation should be granted on the basis of every employee's responsibilities and managed by key allocation. It is vital to ensure that unauthorised individuals cannot get hold of keys at any time, not even for a short while (danger of copies being made). To this end, keys need to be locked away in an approved key cabinet.

Only senior employees have the right to use a master key and/or a passkey; they are also responsible for its safe deposit.

In general, master keys should only be issued to security personnel in case of an emergency. Keys to security-relevant areas must not be issued to cleaning staff.

4.7 Cash deposits

Cash deposits which third parties – if necessary, threatening to use or applying force – could get hold of must be kept at a minimum. A safety container with adequate resistance grade must be provided to enable ticket booth staff to temporarily deposit and/or scoop off large amounts of cash during the day, reducing their exposure. So-called secure safe cabinets (cf. EN 14450) are suitable for this purpose.

The area around the ticket booth should be designed in such a way that quick access to open tills is made as difficult as possible.

Hold-up alarms near the ticket booth staff, and video surveillance, should be installed in the entrance area, taking into account health and safety requirements.

4.8 Video surveillance

Video surveillance systems can only be supplementary to security guards who monitor visitors. As a sole security measure, video surveillance is inadequate (see also chapter 3.4).

4.9 Contractor service providers

Where contractors are hired such as cleaners, transport and/or security personnel, special requirements need to be taken into account.

Consequently, security companies that provide security and supervising personnel should be certified in line with national rules. Companies may offer other services such as gatekeeping certified in line with national requirements for security services.
The responsibilities entrusted to the security personnel need to be defined clearly and unmistakably,

and should be checked for proper implementation.

The security company employed must have adequate third party liability insurance that covers potential loss. The terms of this insurance must be agreed with the insurer.

Only qualified (references) transport companies that are specialised in shipping artefacts should be hired for transport of exhibits within or outside the building.

4.10 Contingency and evacuation plans

Contingency and evacuation plans need to be tailored to the special features of the building as well as the works of art and cultural heritage.

Note: CFPA-guidelines under development. In order to implement loss prevention measures professionally, responses to possible loss scenarios must be prepared. It is necessary to consider what could happen and/or which areas might be affected (cf. chapter 5.5.).

The possible exposure of exhibits as well as possible immediate action should be contemplated. Priorities to save exhibits should be determined. Moreover, it is necessary to create the prerequisites for exhibits to be stored in internal or external storage or to be taken there.

Aids such as tarpaulins, blankets, palettes, packaging material and means of documentation should be provided to permit immediate action to protect and salvage the objects.

Note: In general, it is necessary to bear in mind that it might be necessary to quickly open and/or dismantle partitions and mechanical safeguards in an emergency, e.g. a fire. The appropriate keys and special tools need to be instantly available, which requires a suitable organisation.

4.11 Inventory, identification

All artefacts and collectors' items need to be inventoried collecting the following data:

- Inventory number
- Colour pictures with total views and close-ups of special features such as inscriptions, markings or damage (with scale of colour and dimensions)
- Type of object (e.g. painting or sculpture)
- Description (e.g. shape and colour)
- Material and make
- Size and weight
- Inscriptions and markings such as signature, dedication, title
- Special characteristics such as damaged parts, repair or flaws
- If possible, title of the object
- Subject of artistic expression
- Date of creation, period
- Artist or maker
- Value of the object
- Conservation status
- Restoration measures carried out or planned.

All information and data need to be stored safely to be available after a possible loss of an object. Computer-aided inventory programmes might be a useful option. Any kind of data back-up should be made in a separate room (building) away from the original data.

The data compiled may help to identify stolen or recovered objects, or be useful evidence for police investigations on a theft.

If there are no individual characteristics, or there is no unmistakable description, subsequent labelling may be useful for identification. The label should be clearly visible and attached permanently.

Moreover, labelling by way of special transponders (RFID transponder, Radio Frequency Identification) are also an option. These systems make it possible to save information on miniature storage media directly on the object. RFID transponders are miniature transmitters with individual identification that do not require a power supply of their own. They can be localised and registered by way of scanners. A computer processes the data saved and/or retrieved.

Note: Any lasting change in the artefact or collectors' item has to be discussed with the art experts and restorers of the museum.

4.12 Recovery

Whenever artefacts and collectors' items are stolen, the primary objective is to recover them, which is to say that all possible support must be given to the investigating organisations.

The Art Loss Register (ALR) may help to obstruct sales of stolen artefacts and help resolve art theft. The ALR's data pool is matched with auction houses, galleries and art dealers, thus making an important contribution to resolving crimes involving objects d'art and insurance fraud.

There are representations of the Art Loss Registers all over the world. Further information can be obtained from www.artloss.com.

5 Other recommendations

The following contains some general recommendations for designing, planning and organising a museum. Structural fire protection measures are outlined explicitly in chapter 3.6.

5.1 Exterior lighting

There is no definitive evidence as to the deterring effect of exterior lighting on potential burglars, but it can generally be assumed to exist. Local illumination (lamps, floodlights) increases the risk for a perpetrator of being recognised and consequently caught. Moreover, exterior lighting may be effectively combined with video surveillance technology.

Lamps should be installed and/or designed in such a way that masking or destroying them (e.g. by throwing stones) becomes as difficult as possible. The lights can be switched on by a timer, motion detectors or a dusk switch. Additional lights should be activated by motion detectors in the most exposed areas, so that a potential perpetrator is able to see an immediate reaction to what he is doing.

Sophisticated lighting makes visual inspection of illuminated areas possible. Security guards being blinded by the lights or excessive shadows should be avoided.

5.2 Voltage supply

5.2.1 External electrical outlets

Voltage supply should be restricted to an inner area, i.e. the premises protected by an IAS or security guards. If outside sockets cannot be avoided, they should generally be isolated whenever they are not used – even if they have caps that can be locked. When outside sockets are available, a perpetrator could easily apply electrical tools (e.g. drill, angle grinder), which could drastically reduce the time required to overcome doors, windows, bars or walls.

5.2.2 Backup power supplies

These are recommended so criminals cannot take the opportunity of interfering with the power supply to create a diversion as incover to removing or damaging objects.

5.3 Enclosure

A suitable enclosure constitutes an additional barrier. It might prevent people from getting to the building and make it difficult for trucks to get close to the facade. In addition, the driveway can be blocked by other suitable barriers or bollards, e.g. large natural rocks or planters, even if the premises can not, or should not, be enclosed.

5.4 Increased exposure

Scaffolding outside a museum increases exposure and should be avoided in any case. If scaffolding cannot be avoided, windows that can be accessed from the scaffolding must be protected in the same way as ground floor windows.

Security guards could protect these particularly exposed parts as long as the building is increasingly exposed (i.e. until the scaffolding is removed) as an alternative to mechanical safeguards. Electronic surveillance alone is not sufficient for standard windows because of their low resistance grades. Perpetrators would be able to use standard windows to get inside a building within a matter of seconds.

Note: Wire mesh etc. for plants could be used for climbing; the insurer should be informed about such structures. All windows that can be reached by means of some climbing aids should be protected in the same way as ground floor windows.

Exposure could also be increased by e.g.:

- Installing key storage outside
- Failure or limited function of security systems
- Limited personnel resources in security-relevant areas
- Special exhibits.

The insurer must be informed about the increased exposure; if necessary, the insurer may demand enhanced protection measures while exposure is still high or develop such measures in coordination with the insured.

5.5 In case of emergency

Aside from preventive measures or action that can be taken in an emergency, an evacuation and rescue plan should also specify what to do in case of an emergency. In principle, a timely initiation of rescue measures has a major impact on the scope of damage. This implies:

- In order to avoid subsequent losses (immediately resulting from or fostered by the initial loss), the building affected is to be protected by surveillance and, if necessary, structural measures.
- The rescue and evacuation operations initiated, if possible, during the emergency shall be continued (e.g. moving objects d'art to safe areas that are not affected or alternative storage). Documentation of the objects moved. Unless documentation of losses was not immediately undertaken during the emergency, it should be done in a timely manner.
- If possible, emergency conservation measures should be taken for objects damaged (e.g. freezing soaked books) that prevent further degradation and facilitate subsequent restoration. A plan for such emergency measures must be drawn up.
- Measures that ensure business continuity, e.g. separate areas affected by the damage.
- Targeted public relations activities to avoid possible speculations that could have adverse effects on the museum's image.
- The insurer must be immediately informed and involved in all measures to minimise damage.