Recommendation for the Control of Metal Theft

CFPA-E Guideline No 9:2016 S

CFPA EUROPE

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

1.1 Preface

The damaging impact of metal theft on the communities of the European Union in recent times has become widely known, dating from the sharp increase in metal theft driven by spiralling increases in global metal commodity prices. The costs of metal theft include the cost of replacement and the repair of damage, but there are major indirect costs in addition such as business disruption, customer compensation and loss of revenue.

In the UK in recent times the crime has been estimated by the police to have a total economic cost of about 939 million EUR per year. At one time the demand for copper in the Far East was rising by over 10 percent each month. Naturally the rate of theft will generally track world metal prices which are sensitive to global economic conditions but the implication is that as emerging economies recover and grow the interest of criminals can only increase with time unless effective counter measures are implemented.

The problem is especially challenging because metal is found all around us and is “there for the taking” in industrialised European economies. Indeed one study found that metal thieves travel only between 3 km and 5 km on average and the supervision of disposal channels (scrap dealers etc) has been weak in some member states. Consequently legislators are seeking, and often achieving, stronger metal market and law enforcement controls. The owner of metal assets also has a range of actions that can be taken to contribute to combating the crime and safeguarding the property.

1.2 Scope

This document looks at the problem of the theft of metal, chiefly from in the open or where attached to/forming part of a building and considers the security options.

The security options included in the document are selected in favour of those with significant potential impact on metal theft but the objective here is not to deal with the *general* security of assets against all forms of crime. In the case of a business premises or site the assumption is made that a general security risk assessment has already been completed, possibly with the assistance or input of an insurer, police crime prevention advisor and/or security industry representative. If this is not the case, in-depth guidance on measures such as mechanical protection, intruder alarm systems (IAS), video surveillance systems (VSS, CCTV), access control, perimeter protection, lighting, attacks with vehicles (“ram raids”) and manned security services is freely available from a number of sources such as police crime prevention departments and insurance companies.

Many new security products claiming to be effective against metal theft have arrived on the market. The owner should be cautious before rushing to accept the more “innovative” of these, some of which have a general description in this guide. Many claims are made for security products that are not always supported by independent evaluation. Owners should take care that products that seem to match the general types described in this document actually do meet expectations. “Caveat emptor” (buyer beware)!

1.3 Validity

This Recommendation for the Controll of Metal Theft, 07:2014/7S is valid from 2015, May 1st.

2 References

EN 12320 Building Hardware – Padlocks and Padlock Fittings – Requirements and Test Methods

EN 50132-7 Alarm Systems. CCTV Surveillance Systems for Use in Security Applications. Application Guidelines

IEC 62676-4 Video Surveillance Systems for Use in Security Applications – Part 4: Application Guidelines

3 The Problem

Metal is a quite typical target of thieves. Because of the easy access in most cases a relatively low profit per kilogramme of captured metal is already a very effectual stimulation for perpertrators.

Typically targeted by thieves is metal:

- in the open
  e.g. cable on reels or drums, or actually connected in service and live (electricity supply, telecommunications etc); signs, gates and catalytic converters from vehicles
- attached to, or part of an unoccupied building (particularly if under construction, renovation or demolition or when vacant)
  e.g. roof metal, metal fittings, pipework, tubing, air conditioning plant, lightning conductors, gates, fences, grids, chamber covers, stock
- located in normally unmanned premises/installations
  e.g. sub stations, transformers, wind farm plant
- attached to, or part of, an occupied building or premises (notably premises which are unattended for extended periods such as schools and churches)
  e.g. roof metal, metal fittings, boilers, pipework, air conditioning plant, lightning conductors, gates, fences, grids, chamber covers
- found inside business premises
  e.g. raw material, work in progress, components, stock

Holders of metal in one form or another, particularly non ferrous metal, inside a building have for a long time found it necessary to take special care to ensure that the premises security is adequate. Most of the time, metal thieves see no point in making a lot of effort and so the security precautions already taken by occupiers of such premises may be sufficient, but a review of the security arrangements is recommended.

4 Steps Towards a Solution

4.1 Liaison

Liaison with other interested parties should be considered. For example the landlord and/or an insurer will have a valid interest in the management of crime risk and must to be consulted. Neighbours and police are a potential a source of help.

4.2 Removing/Reducing the Target

As with all business risks the starting point in the risk management process is a security risk assessment consisting of risk identification, analysis and evaluation, including the potential consequences and resulting business interruption and reputational risks. In the case of metal theft it is important to have current information – market prices, crime trends and criminal methodologies. Once the exposure is understood it may be possible to reduce the target and avoid the need to implement countermeasures.

This may be achievable through the removal, relocation or reduction of the metal at risk. One strategy is the use of substitute materials (see below). Another example may be ensuring that materials arrive at agreed times to coincide with installation or that metal stocks are available on demand, avoiding the need for on-site storage. Procedures can be set up whereby metal is ordered in accurate quantities when needed so that surplus is not available on the premises.

If possible, scrap should be out of view and collected frequently to minimise the interest to opportunists. Residual risk needs to evaluated and made subject to controls and protections such as those identified in the next section.

4.3 Substitute Materials

Cable: There are alternatives to copper cable, such as copper coated aluminium or aluminium/tin coated copper, which either have less scrap value, and/or increased scrap processing costs, but thieves may not know the difference so this will probably not deter them in most cases. Caution: such substitutes are unlikely to perform to the same standard as copper cable.

Lead roofing: Of course it may be possible to replace sheet lead roofs with tiles, slates or mineral felt but if appearance and performance similar to lead are desired (or required by a planning authority) the most popular choice is specially coated stainless steel (much less scrap value than lead). Again, due to the similarity in appearance to lead, it may still be attacked (perhaps warning notices on the building would help deter some potential thieves).

There are proprietary roofing systems being marketed as alternatives to lead, but it is not thought that these fully succeed in replicating the appearance of lead.

It is important that the insurance company is consulted about alternative roofing materials in advance, as altering construction materials can affect insurance terms.

Other metal products: Many products taken by thieves such street signs, drain covers, gratings, steps, handrails etc are available in fibreglass or plastic and are almost as durable as iron/steel and with a similar appearance.

Note: Planning permission may be required for certain changes to the appearance of historic premises – check with the relevant planning authority.

5 Primary Prevention and Deterrence Measures

5.1 Networking in the Local Community

The risk can be mitigated through promoting a culture of metal theft crime prevention and criminal intelligence in the local community, especially where neighbours have a similar interest in keeping metal thieves away. Some theft victims report that they have found it difficult to convince the public and the authorities that the problem is a serious risk for the community, employment etc. The true impact on the local community of this crime wave should be advertised.

This starts with networking at senior level with local businesses and owners to encourage awareness and reporting suspicious activity to the police and neighbours – behavior such as “workmen” on a roof without scaffolding or at an unusual time; a cable drum being manhandled into an unmarked van; suspicious persons accessing a cable inspection chamber. Nearly all businesses have metal materials that can be turned into cash so if metal thieves are in the area the whole business community is at risk.

If the community has a local police crime prevention department they can usually provide news and advice.

5.2 Impact Statements in Court

The report presented in any court proceedings that follow an arrest should clearly explain the consequences for the business and community, even though the criminal may not have been able to obtain a lot of money for the metal. A theft of metal of little value to a criminal can have a big impact on a business or community (e.g. a cable theft for which the thief receives just 100 EUR may interrupt a town’s electricity supply for hours!).

Helping the police and courts to understand the importance of what has happened is crucial. Preparation of an “Impact Statement” that explains the full extent of the damage done to the business sends the message that this in not just another property crime without a victim. This should increase the chance that the court hands down a punishment that other criminals will recognise as a real deterrent.

6 Asset Marking and Recovery Systems

6.1 Physical Marking

Marking allows a security operation or the police to trace back any subsequently recovered lost or stolen asset to its original owner. Examples include the attachment of a secure label, embedding an identifier such as a micro dot or continuous identification tape (in a cable), printing or embossing the asset or simply inscribing or etching the asset with characters (e.g. a postal code, name or code word) with an overt or covert marker.

6.2 Forensic Marking

“Forensic marking” generally implies a coding system that, in addition to identifying the legitimate owner or original location of an asset, can link a suspect with the theft in a stronger way than other marking systems; in fact a way that would be more credible in a court of law and assist the prosecution of the criminal.

Such systems generally consist of a medium that itself serves as an overt or covert marker (e.g. a liquid that glows in ultra violet light) in which the forensic code is suspended. The medium alerts the security or law enforcement officer to the presence of the forensic marking. In this example the forensic fluid is sprayed or painted onto assets, but there is also an application when used with triggering devices whereby a suspect is sprayed with the material, and which then links the suspect to the offence – the material remaining detectable on skin and hair for several weeks.

Non-drying forensic “gels” or “greases” which transfer and stick to thieves handling marked assets are also available.

6.3 Secure Database Services

Marking that can not be read and readily linked to the legal owner without reference to records must be supported by a secure database.

Such services should operate to recognised management and security standards. ISO/IEC 27001 specifies high level requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system.

6.4 Wireless (e.g. Radio) Security Tags

This technology, usually associated with items of exceptional intrinsic or heritage value, is used effectively in detection and “sting” operations e.g. to track the illegitimate movements of metal.

6.5 Anti Vandal Paint

Painting external pipes and roofing with non-setting paint, sometimes called “anti climb” paint, deters and hinders access. Occupiers’ liability issues need to be taken into account and suitable warning signs displayed.

7 Passive Security Options

7.1 General

Passive security consists of physical barriers and security devices. For example a fence or the building shell or an item used to secure part of it, e.g. a door lock. There is no active intervention in the criminal event but, instead, the measure is said to “buy time” to allow intervention to take place or for the attack to be abandoned. As well as providing tangible security, passive security acts as a good deterrent. For more Information on so called Perimeter Protection Measures refere to the Security Guidelines Perimeter, VdS 3143 (currently only available in German).

7.2 Site Perimeter

Recognising the amount of force and determination that metal thieves often use a secure pimeter barrier must be provided for metal in the open.

7.3 Fencing

Perimeter fencing should be a minimum height of 2.4 m. High security and maximum security fences should be a minimum of 3.0 m high. The most popular types are:

- Welded mesh fencing: a small mesh size frustrates finger holds and climbing.
- Open mesh steel panel fencing ("expanded metal").
- Steel palisade (vertical steel blades with sharp points at the top to deter climbing).

Notes: Barbed wire or "razor tape" also deter climbing but occupiers' liability issues need to be taken into account and the insurer or legal advisor may require suitable warning signs to be displayed.
Planning permission may be required for certain types of fencing/gates in sensitive locations. Check with the planning authority

7.4 Perimeter Gates

Gates must be of the same height, material and strength as the fencing. Hinges should be designed to prevent the gate from being lifted. Gates are best secured by welded high security proprietary locking bar(s) and padlock(s) to EN 12320, grade 5 or 6.

Where vehicles can approach the buildings, particularly in isolated locations, a "am raid" attack (with a vehicle) must be considered. A purpose designed vehicle barrier such as a trench, high kerb or large concrete obstacles outside the fence, or a series of substantial steel posts just inside the perimeter, can be considered.

Planning permission may be required for certain types of fencing/gates.

7.5 Lighting

If the thief believes that without the benefit of darkness he might be observed lighting can be an effective measure and good deterrent. On the other hand, in a remote, unsupervised location, the presence of lighting may actually assist the thief.

If security lighting is assessed as a cost effective measure, the site, buildings and features should be bathed in a good and even overall level of light. Uneven lighting assists the thief by providing light to work with and shadows to hide in.

Scenes and objects that reflect little light (dark walls, bitumen surfaces etc) will require more light than reflective surfaces.

The deterrent effect can often be magnified by having the lighting facing outwards to "blind" the approaching intruder. This strategy may however be subject to challenge in the local community or through planning law. Check with the planning authority.

Lighting can be switched on automatically by timer and/or photocell but domestic self-contained movement-triggered lighting is to be avoided as it may have erratic performance, is easily interfered with and lacks the deterrent impact of a fixed, continuous installation.

The advice of a security lighting specialist might be obtained. This expertise will help ensure that an optimum and secure installation is achieved using vandal and sabotage resistant lamps, connections and power sources appropriate to the risk level.

7.6 Secure Access Covers

Metal covers in yards, paths and roads are a target for thieves in themselves and/or in order to reach the services (e.g. cable) that they cover.

Lockable access covers are strong covers with robust integral locking arrangements to help prevent opening/removal with simple tools.

Alternatively, secondary security covers increase the time/effort required to gain access to a service chamber using proprietary assemblies secured by special bolts or locks.

7.7 Other Passive Cable Theft Prevention Solutions

There are both in-house and proprietary methods.

Cable/component removal:

- Traditional anchoring methods (a “nut & bolt” approach) or proprietary devices of various types that frustrate the simple dismantling of valuable copper components such as ground bars.
- Cable clamps etc – cable is clamped with purpose-designed security fittings intended to prevent the cable being easily pulled out of the ground or a duct or conduit.
- Welding of access points, burying “pull boxes”.
- Upgraded physical security (e.g. locking components/padlocks) to sub station/plant room/cabinet access points.

7.8 Inhibiting Roof Access

Access to a roof can be hindered by installing barbed/razor wire along roof edges and/or anti climb spikes to external pipes, etc.

Occupiers’ liability issues need to be taken into account and suitable warning signs displayed.

8 Active Security Options

An active security measure is one designed to generate a response to, and intervention in an incident. Examples of active security are the presence of alert staff, a security guard or an electronic security system such as access control, intruder alarm or video surveillance. As well as providing tangible security, overt active security acts as a good deterrent.

8.1 External Video Surveillance

Video surveillance used specifically to tackle metal theft can be an attractive solution in certain cases but the user/specifier needs to be clear as to the objective e.g.:

a) to monitor assets or the approaches/surroundings so that a response can be made if necessary
b) to make a video record of events that could be used by prosecutors in addition to deterring thieves

Obviously one implication of a) is that unless a significant investment is available for the cost of providing an effective observer at all times that the metal is at risk, the investment in the television installation neutralised. And secondly that an implication of b) is that the undetected theft of the metal may still take place. For these reasons “detector-activated” surveillance (see below) is often the preferred solution.

The range of issues that need to be taken into account when making an investment in a permanent video surveillance installation demands competent advice. Installations should conform to EN 50132‑7/IEC 62676-4 Video Surveillance Systems for use in security applications – Application Guidelines.

8.2 External Electronic Intruder Detection

There is a wide range of alarm devices designed for external use such as passive infrared detectors, infrared beam detectors and microwave fence detectors. There are providers that will integrate such devices into an effective external alarm system that would alert a monitoring centre (Alarm Receiving Centre, ARC) who could then summon a key holder and possibly the police (national police rules vary). A more effective solution is achieved when such external detection is integrated with a high quality video surveillance system.

8.3 Electric Security Fence

The following solution may be baned by law in some countries; be sure not to conflict national rights!

An electric security fence consists of a series of tensioned bare metal wires carrying a pulsed high voltage current which is insulated from the carrying posts/mountings.

Anyone in contact with the ground interfering with the fence and touching these conductors, or touching two or more wires simultaneously, will receive a sharp electric shock. The shock is very painful and the thief is obliged to abandon the attack. However it is said that the electric pulse is not physically harmful. Nevertheless this is an "aggressive" device so occupiers' liability issues need to be taken into account and suitable warning signs displayed (usually supplied by the provider).

This solution is usually used to deter or repel unauthorised entry to sites, typically open areas around buildings or storage yards/compounds etc., usually outside business hours. They are most effective when provided with a fence activation sensor (alarm) system; as by this means an alarm can either be sent to on-site personnel or, via a remote signalling intruder alarm or video system, to personnel elsewhere.

These are specialised products, requiring careful manufacture, design, installation and maintenance.

8.4 Detector-Ativated Video Surveillance

Normally implemented in the open, these systems blend intruder alarm technology with video surveillance. They provide flexible and adaptable protection for metal that can not be included in intruder alarm coverage (i.e. typically within the perimeter of the site but not within the buildings) and, being located in a hostile environment, they demand the intervention of a remote operator at a monitoring centre before an event can be notified with confidence to the police or security operation. The system may incorporate a voice warning ("audio challenge") device to unnerve the invader(s).

8.5 Temporary Alarm Systems

Temporary alarm systems are available both for internal and external applications, most being designed to be battery powered only.

Systems usually comprise a portable control/power unit and various wire-free intruder alarm sensors, although some use various forms of audio or visual detection and/or alarm confirmation. Fire detection sensors can be added to some systems.

Most systems provide silent/covert notification of activations to a monitoring centre via a GSM (mobile/cellular) network but some have an option to use additional on-site warning devices. Some products have the option to send periodic test calls to and from site to check the operational status of the system and the means of notification. Notified faults would normally include "low battery".

Temporary alarms are a cost effective and proven way of providing protection against metal theft in selected situations that are without adequate conventional security and/or mains electricity. However, their effectiveness will depend on many factors and competent advice should be obtained.

Even, if no tested and third party-certified product is available, the solution may help to reduce loss on site.

8.6 Underground Cable Theft Detection

Several security solutions have become available in the last few years. Typically they consist of alarm systems that detect when:

A cable chamber or duct is opened:

- A light sensor inside the enclosure triggers the system if daylight or light from a torch or flashlight enters.

A cable is severed or disconnected:

- Fibre optic strand is run, or integrated with, the cable and monitored by a detection device that can detect both severance and its location, and/or, through analysis of sounds and vibrations, detect disturbance of, or close to, the cable.
- Monitoring signal superimposed on live or dead cables detects severance/disconnection.

A security zone established near the cable run is entered or disturbed:

- Buried miniature motion/disturbance detectors and associated cameras watch for movement/shock/vibration.

The method of notifying the alarm condition to the monitoring point with such systems invariably consists of a battery powered radio or GSM transmitter sending alerts/images to the monitoring point, or smartphone or radio network.

Bearing in mind the sheer quantity of cable and the distances they are run (e.g. along a rail line), it is usually only economic to deploy them to a tiny fraction of the asset on a “spot” basis as “trap” protection or as an element of a “sting” operation.

8.7 Roof Access Detection Systems

Church insurers often recommend the use of passive infrared (PIR) motion detectors, similar to those used in Intruder Alarm Systems, fanning out zones of movement detection across the surface of roofing and linked wirelessly to control equipment. These devices are specifically configured for the outside environment in such a way that false alarms from the movements of wildlife are minimised. When the alarm is triggered, strobe lights unsettle the intruder(s) and they may also be unnerved by an audio challenge. Simultaneously an alert is transmitted to a monitoring centre and keyholders are informed.

There are alternative methods also specially designed for roof surveillance:

- One system comprises a detection cable which is secured to leaded areas with a weather resistant, externally rated adhesive. Each zone, terminates in a small wireless transmitter that sends its signals to the control equipment inside the building. Severance or severe vibration will trigger an alert.
- Similar results are given with individual vibration detectors attached to the underside of the roof substrate. Depending on the substrate characteristics and the detector used, each detector can cover a radius of about 2 m.
- As a third example laser detectors shall be named. These products are able to overview a freely defined “virtual surface” within the room. If this surface is being touched by one the will release an alarm.

Challenges given when using any outside-detector are animals and weather. Animals may cause fault alarms which may by treated in the right way. The mayor problem “weather” may cause a temporarily drop-out of detectors. For example during thick fog neither an infrared nor a laser detector will be able to work properly.

8.8 Planning the Intervention

Any intervention initiated by means of electronic equipment or guardsmen or any other kind of third party should be planned and deliberated during the process of rating risks and scheduling counter measures. Even if it seems natural to react to a given alarm from let’s say an intruder alarm system, the way of reaction often is not quite sophisticated or does not leade to an ideal circumvention of loss. It is highly recommended to create an alarm respond scheme in writing and check regularly if every person affected is fully aware of the fixed arrangements – and have the abilities (and rights) to react in respect of those.

9 General Security Measures

9.1 Established Techniques

The enhanced risk of metal theft may call for the reinforcing or supplementing of the security arrangements already in operation. These traditional security solutions may be used or extended to reach one individual goal.

9.2 Access Control

Control of access to metal assets may entail elaborate keyholding arrangements or the presence of human supervision at points of entry. An access control system frequently forms a practical and secure solution through automatically allowing only authorised personnel access without the risks and inconvenience associated with traditional locking or the costs of manned security.

These systems have the incidental benefit of “hardening” the target premises in the perception of thieves, particularly of the type typically involved in metal theft. The advice of a reputable electronic security provider should be obtained.

9.3 Manned Security Services

A human being on site may seem to be the optimum security solution but caution is required. In reality manned guarding is expensive and, if not thoroughly trained, fallible.

Security firms providing guarding services should be approved by the relevant authorities or regulators.

9.4 Intruder Alarm Systems

Traditional intruder alarm systems for the buildings and their contents are well established as a basic building block of business premises security. Certification by the relevant authority or regulator may be required to satisfy the insurer.

Organisations holding metal assets and relying on intruder alarm systems providing modest, general levels of protection may find, in the face of the increased threat, that they need additional detection capability, focused on the metal holdings. The advice of the insurer, security advisor or police should be obtained to ensure the system is adequate in the face of today’s level of metal theft.

10 Maintenance the Defences

The adequacy of the security protection for the assets needs more frequent review than hazards such fire, storm and flood as crime patterns are subject to rapid change through market conditions and social trends. The frequency of these environmental changes is increasing.

Consequently security should must be subject to continuous review e.g. as the nature or value of the assets change, or as crime patterns develop e.g. an increase in the activities of metal thieves in the area. Review is also vital following any security breach or loss.

“Repeat Victimisation” is a familiar criminal pattern. Any revised security measures applied in response to a security breach/loss should be significantly stronger than might have seemed necessary had no previous breach occurred.

The effective operation of the installed security needs to be continuously checked and tested if appropriate. Security solutions must have routine or periodic maintenance to preserve their effectiveness, reliability and credibility.

Finally, the users and operators of the security measures (staff, management, contractors) need to understand the purpose and functioning of the measures and be trained in their correct operation. An adequate introduction to the security measures and suitable initial and ongoing training are essential elements of the implementation of the security strategy.