

UNCLASSIFIED



**D1.1**  
**Physical Security Product Survey**  
***EXECUTIVE PUBLISHABLE SUMMARY***

A report prepared by:  
**Iconal Technology Ltd**  
**FOI**  
**Fraunhofer ICT**  
**Fraunhofer IGD**  
**National Physical Laboratory**  
**TNO**

v1.0

Date: 08/06/2015  
Project No: 606861  
FOI Designation No: FOI-2012-1271  
Dissemination Level: PU (Summary)  
Total No of Pages: 7 (Summary)

---

This project has received funding from the European Union's  
Seventh Framework Programme for research, technological  
development and demonstration under grant agreement no 606861.

UNCLASSIFIED



**D1.1**  
**Physical Security Product Survey**  
***EXECUTIVE PUBLISHABLE SUMMARY***

Version: 1.0 – Executive publishable summary  
FOI designation no: FOI-2012-1271  
Responsible partner: Iconal Technology Ltd  
Author(s): Iconal Technology Ltd: Mike Kemp  
FOI: Jonas Tidström, Anders Elfving, Anneli Ehlerding  
Fraunhofer ICT: Frank Schnuerer, Christian Ulrich  
Fraunhofer IGD: Olaf Henniger  
Morpho: Sebastien Brangoulo  
National Physical Laboratory: Tony Mansfield, Aruna Shenoy  
TNO: Martijn Koolloos, Rinus Gakeer (Bavak Security Group)

Number of pages: 7  
Dissemination level: PU – *Public (Summary)*.  
Start date of project: Sep, 2014  
Duration: 3 years



## Summary

### *1.1 Background*

HECTOS is a European project focusing on harmonization of evaluation, certification and testing of physical security products. Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance, and similar security products are difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality. Currently, there are very few test, evaluation and certification procedures in Europe that are mutually recognized by different Member States. This leads to fragmentation of the market, as identified in the recent EC Communication on Security Industrial Policy, with negative impacts on both suppliers and users.

The HECTOS project focuses on the evaluation and certification schemes for physical security products, and studies how existing schemes used in other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure. Developed evaluation and certification schemes will be validated by applying them to two different product groups as case studies; explosives detection systems (outside of aviation security) and biometric recognition.

HECTOS will result in a roadmap for the development of harmonized European certification schemes for physical security products, and provide standardization bodies with proposals for new work items.

### *1.2 Objectives and scope*

The objective of this report is to provide a foundation for the work of HECTOS by categorizing and describing the different types of physical security product that are used in the provision of physical security solutions and describing their principal characteristics. The aim is to compare and contrast the different categories to support the development of possible harmonised evaluation and certification scheme(s).

The report begins with an overview of physical security products and their categorisation. Each product category is then analysed and broken down into product types together with a description of the key characteristics of each product type.

### *1.3 Physical security*

HECTOS defines physical security as the protection of (mainly physical) assets from physical attack by either criminal or terrorist actors.

Physical security products are defined as physical products (hardware and/or software) that are used in the provision of physical security. Whilst security services are also important and are included by some as a product, in the sense that a service is an output and a repeatable offering from an organisation, services are excluded from the scope of HECTOS.

There is also an overlap between security and safety; furthermore protection from the effects of natural disasters is often within the remit of security agencies. HECTOS does not focus on products whose principal use is safety or protection from natural disasters – although it is



recognised that many products have multiple uses. Finally, there is a wide spectrum of threats that a particular product class might address. For example locks are used on bathroom doors to provide personal privacy in the home; they are also used on vaults in banks used to store large amounts of cash and on security containers used to store classified documents. Within HECTOS, the focus is mainly on the ‘high end’ serious crime and counter-terrorist end of this spectrum.

#### ***1.4 Physical security product categories***

Physical security products can be categorised in a number of ways. The approach taken here is to use a set of categories based on the functions that the products provide as well as taking into account the categories and names used by industry (manufacturers and end-users) in the EU and around the World. Account is taken of the categories used by government security agencies which test equipment for Critical Infrastructure Protection, as well as categories where standards have or are being developed by European standardisation bodies. Other categorisation approaches, such as those based on application areas, such as aviation security products, are considered less useful because many products are used in several different application areas and market sectors.

Physical security is typically provided using a layered approach to control access to the assets which are to be protected. The assets are protected by security measures arranged in layers surrounding the assets e.g. an outer fence, inner fence, building walls, inner rooms, a safe etc. Each layer is protected by **barriers** preventing unauthorised access and entry points where **access management** measures (gates, doors and locks) are provided. **Surveillance** measures are installed to provide situational awareness and assist with command and control of the installation. **Detection** measures may also be installed to detect attacks, unauthorised movements and the presence of prohibited or threat items – these might be intruder alarms, or detectors for weapons or CBRNE threats.

Some products may have functions covering more than one of these categories (for example a safe provides both a barrier and access control through its lock).

This leads to the following set of top-level categories:

##### Barriers

- Fences & Gates
- Building Components
- Vehicle Barriers (Hostile Vehicle Mitigation)

##### Access Management

- Locks
- Safes and Security Containers
- Access Control Systems (e.g. ID card based systems)
- Biometrics

##### Surveillance

- Video Surveillance Systems (also known as Closed Circuit Television (CCTV))
- Security Lighting



#### Detection

- Intruder Detection Alarms
- Chemical Threat Detection
- Biological Threat Detection
- Explosives & Weapons Detection
- Radiological & Nuclear Threat Detection

#### Other

- Secure document destruction

### ***1.5 Product types***

The survey finds that there are a large number of different physical security products fulfilling the various functions described above. They differ in a number of dimensions which may be relevant to evaluation and certification.

#### **Stand-alone, component and system products**

Some products are stand-alone in the sense that a single unit (such as an x-ray machine) provides a significant security function. Even though it may be used together with other products in a security system, the unit has a well defined security functional performance that can be specified and tested

Other products (such as components of a VSS system or intruder alarm system) are combined with a number of other components to form a system and many of the aspects of the security performance depend on the overall system rather than individual components. Access Control Systems are another example of components often sold together as a system, in this case usually by a single manufacturer.

There is also a trend towards integrated security systems. These combine two or more security functions: such as access management, intruder detection, surveillance, perimeter intrusion detection in a single overall system. IT and secure communications infrastructure can be shared and data can be passed between functions to enable more sophisticated processes e.g. turning on cameras once an intruder is detected; tracking credentialed individuals.

Where systems are made up from a number of components, these components may be separate products from different manufacturers, or may be a suite of products designed to work together from a single manufacturer. In the former case, interoperability is very important. In the latter case, which we term system products, interoperability is less important and indeed, the manufacturer may adopt proprietary interfaces in order to provide unique functionality or to ensure that customers buy the complete system from them.

Depending on the functionality of the individual products compared with that of the system and on the way the system needs be designed for each specific application, the emphasis on evaluation and certification may be at the product component level, the system level or the installation/installer level.

#### **Cost and market size**



Products differ significantly in market size, from those where millions may be in use (such as domestic locks) to others where only a handful are sold each year across Europe (some types of explosives detection equipment). The cost of products also varies from a few 10s of Euros up to a million Euros (or more).

### **Maturity**

Physical security products also vary greatly in their level of maturity. Some categories, such as locks and safes generally comprise mature products, with gradual evolution of technology and product types. Others such as explosives and weapons detection include product types with greatly different levels of maturity, from well established walk-through metal detectors and simple baggage x-ray systems, to newly introduced technologies addressing new threats such as bottle screening for liquid explosives, and emerging technologies for applications such as stand-off detection where concepts-of-use are also still at an early stage of development.

### **Application dependence**

Another relevant dimension for evaluation and certification is the extent to which the requirements of different applications of a product type vary with the application. In a number of areas, products are made to meet different levels of security and this is often catered for in standards through the concept of performance grades. With these concepts, the same products can be used in a variety of different applications. Locks and safes are a good example of this. In other areas, variations in the nature of the threat as well as the level of security dictate different types of product for different applications; or, put another way, individual products may have a fairly narrow field of application. CBRN detection products tend to fall into this category.

## ***1.6 Survey structure***

Each section begins with a definition of the product category and the approach taken to categorising the different product types within the category. The product types are then listed and described, with sub-types as well if appropriate. A number of relevant characteristics of each category and type are then given in terms of:

- Product function
- Technology(ies) used
- Application aspects
  - The principal types of user organisation and application area
- Market aspects
  - The maturity, cost and extent of deployment of the products, principal manufacturers
- User aspects

The skills and experience required to design, install and operate systems using the products.



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 606861

The content of this document does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the document lies entirely with the author(s).