HECTOS

Harmonized Evaluation, Certification and Testing Of Security products

D5.5
Summary of findings from the Weapons & Explosives detection case studies and their implications for harmonised certification schemes

EXECUTIVE PUBLISHABLE SUMMARY

A report prepared by:
TNO
FhG-ICT

Date: 2017-04-19
Project No: 606861
FOI Designation No: FOI-2015-1958
Dissemination Level: PU(Summary)
Total No of Pages: 6

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

HECTOS

D5.5
Summary of findings from the Weapons & Explosives detection case studies and their implications for harmonised certification schemes

Version:	1.0 – Executive Publishable Summary
FOI designation no:	FOI-2015-1958
Responsible partner:	TNO
Author(s):	Martijn Koolloos, Erik Kroon (TNO) Christian Ulrich (FhG-ICT)
Number of pages:	6
Dissemination level:	*PU – valid for the Executive summary*
Start date of project:	September, 2014
Duration:	3 years

HECTOS

Executive Summary

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 (MS). 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. By conducting two case studies in the priority areas “Biometrics” and “Weapons and Explosives Detection” HECTOS will enhance, and experimentally investigate elements of the evaluation and certification framework that is developed within the project.

The objective of this deliverable D5.5 is to analyse and assess the evaluation processes and outcomes for the W&E detection case studies “Explosive Trace Detection (ETD) Products” and “People screening portals” as reported in D5.4 Part I and II against the elements of the certification scheme outlined in D3.3. This results in recommendations to enhance the viability of a harmonised certification scheme for this type of security products.

The main common and case-study specific conclusions from these two case studies are:

Common findings and recommendations for W&E detection products

- Given the complex nature of the evaluation and the societal relevance of security, the scheme for W&E detection products certification should concern type certification and include a site acceptance test, periodic surveillance testing of products and periodic audits of the management system of the manufacturer (Type 5).
- The test method for W&E detection products is primarily aimed at assessing the detection rate (DR) and false alarm rate (FAR).
- For a product category a high level general TM may be defined. For a product type, a process is needed to determine whether the proposed TM (e.g. from another product type) is suitable or should be adjusted (and how).
- The TM should be comprehensive and include all possible parameter that may be needed for certification. The TM should include these levels of granularity with sufficient statistical confidence.
- The statistical validity should be defined in the certification scheme. The required confidence intervals of the test results (both overall and at higher levels of granularity) should be determined in the scheme and the test method should give instructions on how to calculate the corresponding number of test runs.
- Test-induced variance may be larger than the statistical variance especially for TMs where human beings are involved (either as a test person or as a tester with a potentially large influence on test parameters).
- Test results can be used for conformity assessment against detection performance requirements that depend on the application area. Certification can hence be done for more applications.

HECTOS

- A high level general description of the TM for Explosives and Weapons Detection devices should be unclassified in order to enhance harmonization distribution (also to manufacturers) and recognition of the TM.
- Threat items and amounts to be tested should be classified only for high-security applications provided that they can be revealed to the stakeholders on a need-to-know-basis. At lower security levels they might be unclassified.
- Multiple performance grades are possible and the way to implement them in a certification scheme depends on the product type.
- The HECTOS framework should acknowledge the classified nature of requirements related to “explosives and weapons detection”. The limited availability of requirements may negatively affect the harmonization and/or recognition of the scheme.
- Scheme owners, scheme operators and test bodies need to have access to these requirements to enable conformity assessment.
- The requirements for detection performance evaluation can be conflicting in terms of the threat items to be included in the test (the so-called short list). Every country can have its own priorities with respect to threat items, based on a national risk analysis. The requirements should specify the threat materials and should be determined by the members of the scheme owners. When requirements are defined as European regulation they should be defined as a long list, categorized in threat groups. The TM can then be an “exam” with an agreed short list. If national authorities want more stringent requirements, these should be included in the harmonized standards but possibly in the form of additional performance grades.
- The costs for a certification test for W&E devices are generally high and should be included in the business case of the scheme.
- Security performance evaluation of W&E detection products is not suitable for self-testing by the supplier, mainly due to classification issues. A combination of self-testing against existing public standards and a comprehensive test for security performance assessment by an accredited test lab may be a good combination that should be assessed for each product group.
- Re-use of evaluation results is only possible for explosives and weapons detection products that are capable of recording raw data. A correct registration of all runs during the test is a prerequisite. The TM must include a dedicated part for re-testing based on raw data captured during a previous full test of the same configuration, but with a different detection algorithm.
- For each W&E detection product / application it must be assessed whether the outcome of the performance tests contains classified data (detection rates for specific threat items). If so, the results cannot be published publicly. However, the outcome can be used by the appropriate authorities for conformity assessment and these results can be published without restrictions.
- Laboratory consistencies can be obtained by regular inter-lab visits of the test houses during testing to learn from each other and to assure that the test is performed correctly.
- A certificate is valid only for the configuration (hard- and software) that has been tested. Any change to the configuration will lead to a withdrawal of the certificate unless the certification body determined the changes to be uncritical to the performance.
- The validity of a certificate can furthermore be limited for a time period, after which a reduced test has to be passed to renew the certificate.

HECTOS

- A new certificate can be issued after re-evaluation. In case of a new detection algorithm a re-play of the raw data with the new algorithm might be sufficient, if critical changes of hard- or software have been made or the requirements are changed a full retest has to be done.
- A periodic surveillance test programme (reduced full test) should be designed to guarantee a system under permanent operation still fulfils the requirements.

Specific findings and recommendations for ETD

- A general TM for ETD can only be defined on a high level by defining the test blocks:
  - Threat detection test
  - False alarm test
  - Suppression test
- For each product type (swab-based particle sampling-, optical-, vapour phase-, etc.) the details of the three test blocks must be specified individually. As a consequence of the complexity to gain valid trace samples, a two stage evaluation has to be considered. In the first stage only valid but artificial samples, which can be prepared with a high accuracy are tested. In a second stage more realistic samples will be tested, which intrinsically cannot be prepared with the same accuracy.
- System specific characteristics, for example false alarm on solvents when testing volatile substances, have to be determined in a scoping test.
- Threat-identification increases the trust in the result, but holds the risk to overestimating the detection capacity of non-identifying systems.
- Adversarial testing has to be defined accurately and can be done for example by masking threat substances by a huge amount of interfering substances or by overloading the system with high concentrations of target substances.
- The repeatability of security evaluation of ETD can be improved if the following parts are included in the test protocol:
  - Exclude solvents that cause false alarms for testing of volatile compounds;
  - Sample preparation and measurement for non-volatile compounds have to be performed on the same working day;
  - The use of single source test materials is mandatory.
- Testing only samples which can be prepared with a high accuracy will improve the repeatability. A meaningful testing will however require additionally more realistic samples with a lower repeatability.

Specific findings and recommendations for people screening portals

- The following level of granularity should be included in a TM for people screening portals: gender, BMI, threat type / size / location, level of divestment.
- Scoping tests should be used to determine the regions (combination of threat type/size, location and sensitivity of the detector) where the detection system has sensible performance. Testing efforts can then be focused on those regions and wasting time on regions where the performance is virtually zero or virtually perfect can be avoided.
- Alarm zone indication is optional and depends on the envisaged ConOps. It may be taken into account when it is accurate, otherwise the device should be considered a binary detection system (alarm / no alarm).
- Adversarial testing for the people screening portal evaluation can be done by: using test persons instead of automatic frames and allowing deviant human behaviour during

HECTOS

scanning, applying different levels of divestment, and carrying simultaneously threat items and benign items.

- For people screening portal test methods where test persons are involved, the following ethical issues must be addressed:
    - When real explosives are part of the TM, and these explosives are attached to the test persons, it must be clearly stated in the test protocol that their participation is strictly voluntary and people cannot be forced to participate
    - Since images and personal information are recorded, all appropriate EC privacy and data collection regulations shall be obeyed.
    - Because of the previous points a clear “Informed Consent Form” must be developed in the mother tongue of the participants and be signed by each participant.
- A high repeatability of security performance tests for W&E detection products can be obtained when one or more of the following measures are included in the test protocol:
    - A large number and wide variety (gender, BMI) of test persons (≥16)
    - Prescribed type of garment
    - Prescribed location, orientation and concealment of the threat item.

  The effectiveness for the repeatability on these measures must be investigated in order to develop a good TM.
- Most people screening portals are large and vulnerable and are not built for transporting and installing on a regular base. Therefore, frequently installing and disassembling the same machine in two or more labs for proficiency testing is not feasible.