PROJECT FINAL REPORT

Grant Agreement number: 217872

Project acronym: IDETECT4ALL

Project title: Novel Intruder Detection & Authentication Optical Sensing Technology

Funding Scheme: Collaborative project

Period covered: from 01/07/2007 to 30/06/2011

Name, title and organisation of the scientific representative of the project's coordinator[1]:

John Morcom, Managing Director, Instro Precision Limited

Tel: +44 (0) 1843 604455

Fax: +44 (0) 1843 861032

E-mail: johnmorcom@instro.com

Project website[2] address: http://www.idetect4all.com/

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the grant agreement

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm ; logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

Table of Contents

1. Final Publishable summary report 3
1.1 Executive summary 3
1.2 Project context and objectives 4
1.3 Main S&T results 8
1.4 The potential impact 23
1.5 Public project website - www.idetect4all.com 34
1.4.1 Competiveness 23
1.4.2 Ethical issues – data protection and dual use 24
1.4.3 Socio-economic impact and the wider societal implications 25
1.4.4 Dissemination & Exploitation in iDetecT4ALL 26
2. Use and dissemination of foreground 39
2.1 Section A 39
2.2 Section B 40
3. Report on societal implications 42
Part B1 40
Part B2 41

Table of Figures

FIGURE 1 – TABLE OF PRODUCT 10
FIGURE 2 – 5 END USER OPERATIONAL SCENARIOS 12
FIGURE 3 – ARCHITECTURE OF IDETECT4ALL SYSTEM 13
FIGURE 4 – FULL INTEGRATION OF THE SYSTEM PROTOTYPE AT IPL, BROADSTAIRS, UK 17
FIGURE 5 – FIELD TRIAL PROTOTYPE IN FIELD TESTING 18
FIGURE 6 – SENSORS 26
FIGURE 7 – SENSOR'S INSIDE 26
FIGURE 8 - PROJECT BROCHURE (SPANISH) 30
FIGURE 9 - IDETECT4ALL PROJECT POSTER & FIELD TRIAL POSTER 31
FIGURE 10 - IDETECT4ALL LIEGE FIELD TRIALS FOLDER 32
FIGURE 11 - IDETECT4ALL PEN DRIVES & PENS FOR THE FIELD TRIAL EVENT 33
FIGURE 12 - IDETECT4ALL FIELD TRIALS VIDEO 33
FIGURE 13 – IDETECT4ALL WEBSITE 34

1. Final Publishable summary report

1.1 Executive summary

- Novel Intruder Detection & Authentication Optical Sensing Technology

The objectives of the iDetecT4All project were to research and develop a low cost security sensor technology and demonstrate its use as part of a complete system suitable for protection of critical infrastructure.

A key driver for the project was to overcome the high cost and unacceptable false alarm rates that limit the deployment of existing security sensor technologies.

The core technology of the project, a multi-pixel optical time of flight based approach, was researched and developed to deliver working prototype sensors with the ability to both detect intruders and remotely scan and read optical tags worn by authorised personnel/vehicles.

A security system architecture was defined to capture sensor alert event data, transmit it to a remote control centre and then slew an imaging system to view the intruder event.

A prototype communications network, based on open standards to minimise cost, was developed to transport the event messages. A “back-office” database was created and linked to control centre application software and a Geographic Information System to correlate sensor alerts. A high resolution imaging system was also developed with an internet control protocol to accept sensor alerts and slew to view the detected event.

Unforeseen problems associated with the complexity of the sensor technology caused a delay in the sensor development but these were overcome and the delay mitigated through careful planning and co-operation within the consortium.

The whole system was integrated and then tested in the field at Faro and Liege airports using representative critical infrastructure protection scenarios. A wide variety of test cases were examined including authentication and detection of walking and running personnel and vehicles . Tests were carried out both day and night and in adverse weather conditions such as heavy rain.

The field trial results demonstrated that the sensors and system delivered useful levels of real world performance and confirmed that the main project objectives of achieving a very low false alarm rate and high detection rates had been achieved. Detailed analysis of the raw sensor data indicates that there is scope for further improvement of the sensor performance through additional optimisation of the hardware and signal processing algorithms.

A key technological breakthrough was achieved with the development and demonstration of a single sensor able to both detect intruders and also authenticate personnel and vehicles by reading remote optical tags.

It is believed that with suitable levels of investment in optimisation and then engineering for production, such a sensor and the associated system could be deployed to improve protection levels at critical infrastructures in the European Union and the World.

1.2 Project context and objectives

Introduction

The objectives of the iDetecT4All project are to research and develop a low cost security sensor technology and demonstrate its use as part of a complete system suitable for the protection of critical infrastructure.

A key goal of the project was to overcome the high cost and unacceptable false alarm rates that limit the deployment of existing security sensor technologies. To achieve this, the iDetecT4ALL project was based on an innovative optical sensing technology with the potential to deliver cost effective protection for many different types of critical infrastructure installations.

Unlike the majority of low cost sensors available on the market today, this Active Matrix Ranging (AMR) sensor technology uses a physical measurement of the presence or absence of an intruder to deliver a very low false alarm rate. A further unique aspect of the AMR sensor is its ability to differentiate between authorised personnel/vehicles and intruders by remotely scanning and reading a tag worn by authorised personnel/vehicles.

Approach

To ensure the project remained aligned with “real world” security considerations, an important aspect of iDetect4All’s approach was the formation of a multi-disciplinary project team that included security specialists and end users (airport operators and police & fire brigade emergency response centres) as well as technology development partners.

The project work was divided into the following phases:

a) Review of end user requirements;
b) System architecture definition;
c) Technology research and development through to prototype design and manufacture;
d) System integration;
e) Field Trials; and
f) Analysis and evaluation.

In parallel, a dissemination activity informed the security community of the progress of the project through the iDetect4All web presence and attendance at appropriate conferences and meetings.

An ethics committee was constituted to review the ethical considerations associated with the system. The work of the ethics committee also informed and drove the selection of appropriate methodologies for conducting the field trials.

Project Work

Discussions with end users identified a series of typical operational scenarios associated with delivering critical infrastructure protection. From these different operational applications, a common set of sensor functions was defined that could apply to the diverse set of scenarios. In addition, a set of field trial evaluation criteria was defined to enable validation of the sensor and system performance in terms that would be meaningful from a critical infrastructre protection perspective.

Consideration of the system architecture lead to a system concept whereby AMR sensor detection events arising from authorized and unauthorized intrusions are relayed to a central control centre. Here the detection event information is fused with a Geographic Information System (GIS) to cue an “Alert Tracking & Observation Sensor” (ATOS). This provides the system operator with a high resolution visual and infrared image of the event area along with precise location information. The operator can then make an immediate assessment of the situation and, if necessary, deploy additional security resource to the event location.

The AMR sensor technology research and development commenced with the generation of performance models for the sensor and tag. These models were then used to determine the optimum design concepts for the optical sensor and tag.

Unfortunately this phase of the work took longer than anticipated as the design trade space was found to be larger than originally envisaged at the start of the project. To overcome these delays, sensor simulators were

provided to allow the development and integration of the other system elements to proceed.

Nonetheless, the modelling work provided a very useful insight into system optimisation and gave a good degree of confidence in the sensor and tag design concepts selected for development. Hardware and software development of the AMR sensor was then completed and required a mix of low noise, wide bandwidth analogue circuit design, digital signal processing and optical design.

Significant challenges addressed during included the implementation of a multi-channel parallel digital signal processor in a field programmable gate array (FPGA) to achieve the required sensor frame rate. As shown in these photographs, critical elements of the design were prototyped in an open chassis form to allow their performance to be evaluated and optimised prior to incorporation in the final prototype enclose.

A generic tag emitter was designed and integrated into both standard vehicle warning beacons and high visibility tabards as worn by security personnel around critical infrastructure areas.

Both sensor and tag performance parameters were measured under laboratory conditions to validate the sensor and system modelling assumptions.

Development of the alert tracking and observation sensor (ATOS) was also carried out successfully. Careful consideration of the design trade-offs yielded a high performance and cost effective solution based on an uncooled thermal imaging module with optimised lens assembly.

An internet protocol based control system was also developed to allow the ATOS to accurately respond to the control centre alerts.

An important part of the overall system was an efficient, low power yet flexible communications system to relay messages from the AMR sensors to the command and control centre.

Particular challenges in achieving this requirement arose because of the distributed nature of critical infrastructure and the need identified by end users to be able to set up protection on an ad-hoc basis.

To address this, a multi-modal communications system was developed based on existing technologies such as Wi-Fi, GPRS/EDGE and high speed commercial internet (HSPA) links. Wi-Fi was used to create an ad-hoc network to link distributed sensors to a master communications control unit (MCCU). The MCCU then used HSPA to transport the sensor events to the remote command and control centre. As a backup communication channel, a GPRS/EDGE direct link was used from the CCU units to remote command and control centre when no HSPA network was available for MCCU.

The prototype communications links were tested in a wide variety of deployment conditions (urban and rural) to verify their performance and reliability.

System Integration

Following completion of the design and manufacture of the hardware elements, they were integrated together to prove the “end to end” operation of the complete system.

The integration work included the development of a “back office” server to process event messages delivered via the communications network. A command and control application was developed to interface with the “back office” and a geographical information system. The command and control application contained algorithms to correlate the event data from adjacent sensors and allow the operator to see the location of the events plotted on a map. The application software also issued commands to the ATOS to slew its line of sight to the location of the event, providing a high resolution image to the operator.

Field Trials

Field trials were carried out at FARO Airport and the LACHS cargo terminal at Liege. These two locations were chosen as being representative critical infrastructures.

Five specific test scenarios were selected for the trials including:

a) Virtual Fence: i.e. protection of a perimeter

b) Aircraft Parking: i.e. ad-hoc protection

c) Baggage Cart protection

d) Indoor Air cargo protection

e) Outdoor Air cargo protection

These scenarios were divided between Faro and Liege as illustrated in the diagram above and the practical field trials were carried out during Q1 of 2011. For each test scenario, many separate test cases were defined and examined including vehicles crossing and stopping within the sensor field of view and personnel walking and running across the field of view. Tests were made both with and without tags on the subject vehicles and personnel. In addition, each test case was carried out in the daytime and at night.

During the final field trial at Liege, the complete functionality of the system was demonstrated to the Project Officer and Reviewers and the high detection rate was observed.

A substantial amount of raw sensor data (many hundreds of gigabytes) was captured by the prototype AMR sensors during the field trials together with detailed records of the test scenarios and results.

A detailed analysis and review of this data allowed the performance of the sensors and system to be quantified in terms of false alarm and detection rate parameters as required for evaluation of a critical infrstructure protection system.

Results

The field trials showed that the prototype sensors and system delivered a very low false alarm rate and high detection rate, confirming achievment of one of the key goals of the project.

It was noted that on a small number of occasions a tagged individual was detected as an intruder. This was attributed to the tag emitters occasionally being hidden from the sensor by the individual's arms as they walked or ran. However, this was not considered a major issue as all the intrusions is detected. For future systems this could be addressed with different placement of the tags on the tabards.

Detailed examination of the raw sensor data indicates that with some sensor hardware improvements and modifications to the detection algorithms, even better detection rate performance could be obtained.

iDetecT4ALL consortium

The iDetecT4ALL consortium brings together 10 partners from 7 countries, each partner brining its own unique expertise to the project. The partners have built a strong and balanced consortium, including SMEs, large industries and end users.

Beneficiary name	Short name	Country	Contact person
Instro Precision Limited ***– Project coordinator***	IPL	UK	Mr. John Morcom johnmorcom@instro.com
Motorola Israel Ltd.	MIL	IL	Boris Kantsepolsky Boris.Kantsepolsky@motorolasolutions.com
Everis	EVR	ES	Mario Carabaño Marí Mario.Carabano.Mari@everis.com
C.A.L. Cargo Airlines	CAL	IL	Avishay Gazit avishayg@cal.co.il
3D s.a.	3D	GR	Odysseas Spyroglou ospyroglou@dotsoft.gr
A.N.A. Aeroportos de Portugal	ANA	PT	Edgar F. Carvalho EFCarvalho@ana.pt
Liege Air Cargo Handling Services	LACHS	BE	Avi Yehene AviY@cal.co.il
Azimuth Technologies Ltd	AZI	IL	Kfir Adam kfir1959@gmail.com
S.C. Pro Optica S.A.	PRO	RO	Dan Ursu dan.ursu@prooptica.ro
ARTTIC Israel International Management Services 2009 LTD	AIL	IL	Moran Naor naor@arttic.com

1.3 Main S&T results

At project level

Following the second and final year of the iDetecT4ALL project the consortium has achieved all of its stated overall goals and developed a system consisting of a number of applications which have been integrated to one working system, tested and demonstrated within the project, proving the feasibility and success of the iDetecT4ALL project. The following research and technological development activities have been carried out throughout the project:

iDetecT4ALL's professional services are outlined below:

1. Sensing and ID tagging technologies

- The Design and specification of the sensor and tag according to the user requirements was done in the 1st period of the project and the results were presented in D3.1 iDetecT4ALL Sensor and OPID Tag design.

- The main design goals were achieved on the 2nd period of the project in the hardware development phase of the iDetecT4ALL sensor and OPID tag. The prototype was first presented to the consortium in the field trials in Faro, Portugal and was also presented in D3.2 Prototype of ID2 sensors and tags.

- After producing the prototype it went through a series of lab tests and measurements which were presented in D3.3 ID2 sensors and tags lab test summary report. The tests performed confirmed that the hardware worked as expected

2. Alert Tracking Observation System (ATOS)

- The Design and specification of the Alert Tracking Observation System according to the user requirements was done in the 1st period of the project and the results were presented in D4.1Alert Tracking Observation design report.

- The main design goals were achieved on the 2nd period of the project in the hardware development phase of the ATOS. The prototype was first presented to the consortium in the field trials in Faro, Portugal and was also presented in D4.3 Alert tracking Observation Prototype.

- After producing the prototype it went through a series of lab tests and measurements which were presented in D4.2 Alert Tracking Observation Lab report. The tests performed confirmed that the hardware worked as expected

3. Communicate System

- The Design and specification of the communication system according to the user requirements was done in the 1st period of the project and the results were presented in D5.1 communication system design.

- The main design goals were achieved on the 2nd period of the project in the hardware development phase of the Communication system. The prototype was sent to IPL for the test labs and was presented in D5.3 MCCU/CCU prototype Description

- After producing the prototype it went through a series of lab tests and measurements which were presented in D5.2 MCCU/CCU Lab Test report. The tests performed confirmed that the hardware worked as expected

4. Command and Control Center

- The Design and specification of the communication protocols between the Command and Control Center and the ATOS and the CCU/MCCU were initially done in the 1st period of the project. The protocols and the results of the lab integration were presented in WP5.

- The main design, implementation and the accomplishment of goals were achieved on the 2nd period of the project in the software development phase of the Command and Control Center.

- The prototype of the Command and Control Center was first presented to the consortium in the Field Trial Prototype on December 2010 in Israel. After that the Command and Control Center participated successfully in the field trials at Faro Portugal on February 2011 and in the proof of concept demonstration of iDetecT4ALL system that took place at Liege International on March 2011

5. **Integration –** Integration has been a primary focus of the second reporting period, with several integration sessions taking place throughout the year:
    - The integration activity (WP6) has started with D6.1 Integration Plan, the integration plan contained:
        - Definition of all system integration efforts.
        - Preparation for integration phase.
        - Integration phase structure.
        - Expected outcome.
        - Schedules.
    - After all the technological components had been developed by the technological partners the field trial prototype system was integrated . The system prototype was presented in D6.2 field trial prototype system.
    - The Integration process was made in a few levels.
        1. Integration between communication system and the sensors and ID tags.
        2. Integration between Command and Control Center (CCC) to Communication system and sensors and ID tags.
        3. Integration between CCC to ATOS.

6. **Field Trial –** A field deployment of the iDetecT4ALL system was executed in 2 different locations throughout the 2 period of the project, Faro airport in Portugal and Liege airport in Belgium.
    - **All applicati**ons functioned in a satisfactory manner in the field trials.

The product

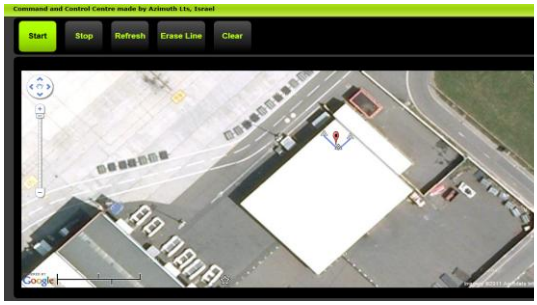
iDetect4ALL's product is comprised of a technology which detect the presence of objects (human beings, vehicles, goods), inside or in the surrounding area of restricted critical infrastructures. iDetect4ALL is a **sophisticated intruder detection system** based on an innovative photonic sensing technology which deploys ultra-low cost electro-optical components.iDetect4ALL implements an end-to-end security application by integrating:

1. An array of ID2 sensors, capable of detecting intruder objects and reading the optical ID (OPID) tags within the field of view.
2. ID tags (for identification) which are attached to authorized objects.
3. Server hosted situational awareness algorithms and software capable of alerting predefined threats and monitoring them.
4. An electro-optical alert tracking observation module that is directed to any unauthorised object detected, and used to track and observe the object being identified as a potential threat.
5. A threat alerts display for command and control centres.

6. Low cost communication and networking units for product component interconnection.

Figure 1 – Table of product

Item	Description	Illustration
SENSORS	N sensors that can form a restricted area (virtual fence or perimeter). The sensors have an integral power source and communication module that enables the user to configure the unit, test it, align it and operate it.	
ID TAGS	M tags that are distributed to the authorized users. The user identities are registered at the command & control (CC) centre of the CI.	
ATOS	Observation system that includes a pan and tilt module carrying a day and thermal image camera. This unit is connected to the CC centre of the CI and delivers real time video information. It enables the user to track the intruder and provides the ability to control camera functions features.	
Communication system	A new and unique for Idetact4All CCU and MCCU communication system units were developed and introduced to demonstrate a simple for installation, cheap for maintenance and reliable in different environmental conditions communication solution for Idetact4All applications.	 **CCU Front view**

		MCCU Front  **view**
Command and Control Center (CCC)	Web based system including a tailored application for surveillance and intruder detection. It includes database management and event management capability to help decision making and intervention team activation. The CCC includes a communication module that enables the CCC to monitor the sensors that form a restricted zone and get information from the sensors.	 Command and Control Center

At WP level

WP1

WP1 was dedicated for the analysis and definitions of the End User Requirements (EUR) for the detection and reporting of unauthorized intrusions of human and vehicles into restricted areas within EU critical infrastructures and then transform these EUR's into use cases and operational scenarios (as described in D.1.1).

Each one of the end user partners (ANA, 3D, EVR, LACHS and CAL) provided its different security objectives and operational requirements. Furthermore, each of these partners had a different role within a critical infrastructure operational environment, and each of these partners represented a different type of critical facility. Those varieties of different security objectives and different operational requirements assured that the iDetecT4ALL System will provide a robust security solution to address the diversified needs of various types of critical infrastructures.

Following by the achievements of the above WP1 objectives and tasks the five (5) use cases and operational scenarios (D1.2) were used by AZI as the guidelines for the iDetecT4ALL technology architecture and system development (WP2) and for the Field Trial Prototype specifications (WP6), followed by the Field Operation Trials (FOT) as defined in WP7, and during the execution of the Proof of Concept Demonstration (PCD) as defined in WP8, and finely as reference criteria's for the overall evaluation of the iDetecT4ALL system (WP9).

The following are the five user scenarios that were defined at WP1 and later tested at WP7 and WP8:

	Test description
Scenario A	A large fenced external perimeter that circles all critical infrastructures
Scenario B	A remote area for Aircraft parking which corresponds to Permanent Virtual Fence with Limited Access
Scenario C	Outdoor checked baggage storage, Provide coverage of enclosed baggage carts at a temporary outdoor storage location within an airport restricted area.
Scenario D	Indoor Cargo Storage, Provide coverage of enclosed air cargo pallets that are located within an indoor cargo storage facility
Scenario E	Outdoor Cargo Storage, Provide coverage of enclosed air cargo pallets at a temporary outdoor storage location within an airport restricted area.

Figure 2 – 5 End user Operational Scenarios

Significant results to be mentioned for WP1 are:

1. Identification of unauthorized access of human and vehicles into permanent restricted areas
2. Identification of unauthorized access of human and vehicles into ad-hoc restricted areas
3. Friend & Foe (FF) identification - Distinguish between authorized access and unauthorized access at the above restricted areas
4. Provide the MOST realistic 5 use cases and operational scenarios – enable the design, test and validation of iDetecT4ALL system

WP2

The objectives of WP2 were:

a) To research the topology and integration architecture of the main technology components (Sensing, ID, Alert Tracking, and Networking) to provide an optimal solution for the User Requirements as specified at WP1. To explore various technology parameters and trade-offs.

b) To specify a field trial prototype system that will implement an end-to-end threat detection security system, based on the developed technologies for intruder detection, optical tag reading and object authentication and alert tracking observation, that will enable to display and validate, under real world conditions, the project out-come.

c) To specify the selected Architecture, it's sub-technological modules and any other means that are needed for the Field Trial Prototype of end-to-end solution.

All of the work package objectives were met while keeping the schedule presented in the DoW.

The system architecture and topology were defined and designed to meet the end users' requirements.

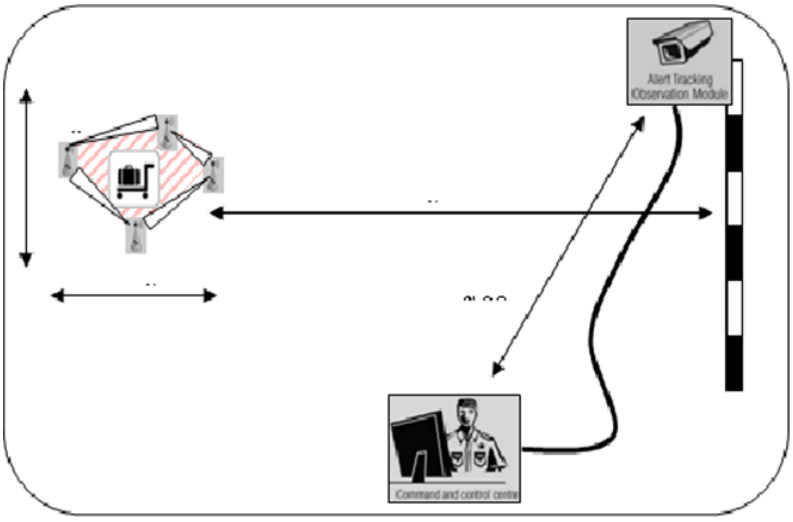
The research of the topology and the architecture was done by technical partners:

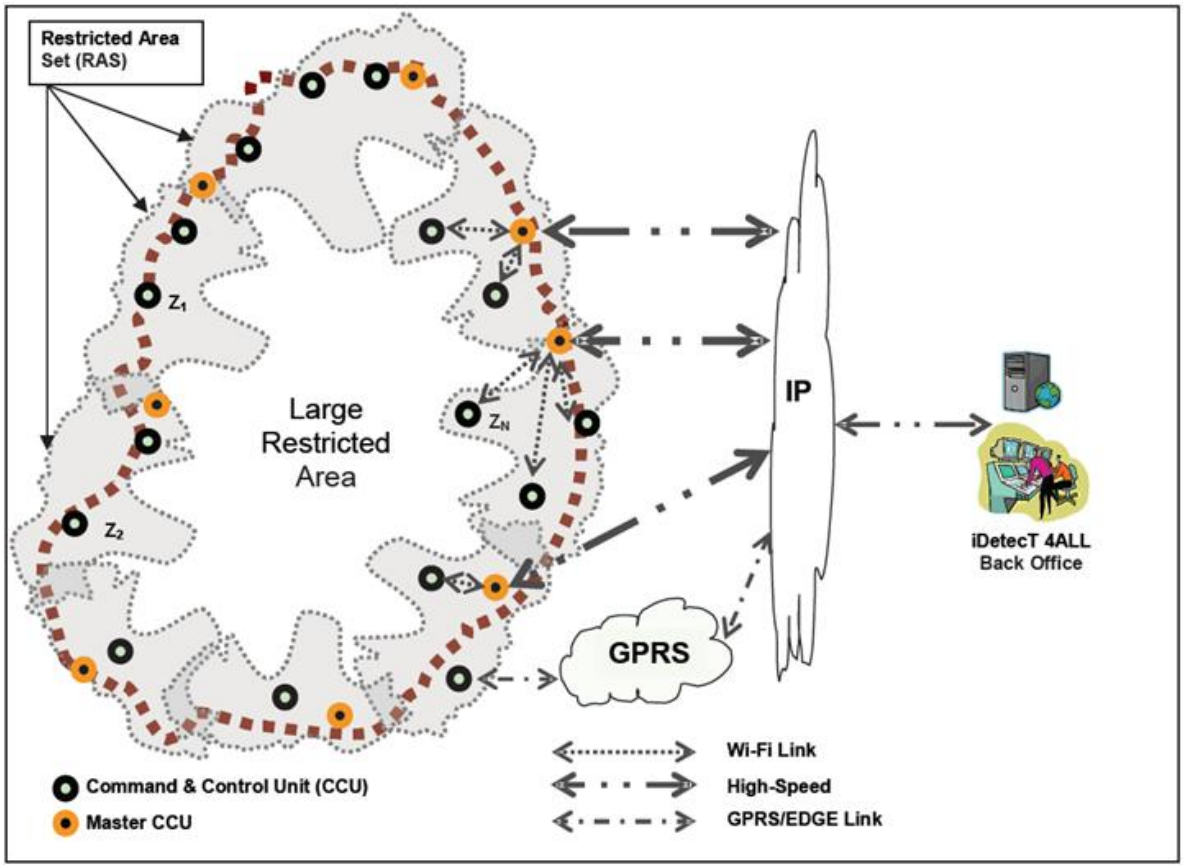
- Sensing and ID Tagging Modules Mathematical modelling analysis was done by IPL.
- Alert Tracking Observation Module simulative model was done by PRO.
- Communication architecture options were done by MIL.
- Application layer processing architecture was done by AZI.

The Field Trial Prototype system was specified including;

- The definition and split of functionalities between the system blocs.
- Interface definitions of the various modules.
- Performance specifications for each of the models.

Figure 3 – Architecture of iDetecT4ALL system





WP3

The purpose of WP3 was to research and develop; optimise optical sensors and tags for the iDetecT4ALL system with the objective of meeting the target sensor and tag specifications determined during WP2. To design, manufacture and carry functional lab test for prototype needed for field trial Prototype system. To work with Azimuth, Pro and MIL to ensure the prototypes are compatible with the system architecture and communications methodology.

All objectives were met during this Work Package. A sensor system was designed and built to meet the specifications set out in WP2. These were tested in the Lab, and successfully deployed in Field trials to detect intrusions.

The six systems were completed in time for field trials at Faro Airport in February 2011. They had been built and tested at Instro Precision Limited and provided data sufficient enough to build confidence in their operation and detection capability.

Whilst in the real world environment of the Faro field trials and Liege proof of concept trials, the systems performed well. The systems consistently detected intrusions and were able to differentiate between friend and foes. These positive results provided the feedback for assessing the design and build work undertaken in WP3.

The only deviation that impacted WP3 was time. The development of the sensor and tag systems was six months late due to the initial concept not being suitable for implementation on multiple sensor deployment. Unfortunately, this required that the development of a new concept was required and therefore a delay was inevitable.

WP4

The Alert tracking observation system (ATOS) is a module with a relative high degree of independence inside the iDetecT4ALL system.

Despite of this independence, parameters defining the ATOS functionality are determined by the requirements for the all system.

After a relative long period need to establish user requirements discussions regarding some ATOS features were carried out:

- the role of the laser range finder capability of ATOS in the iDetect4ALL functionality;
- the ATOS communication with the Command and Control Centre (CCC) as the part of general iDetecT4ALL communication;

Regarding second problem, at the consortium level was decided that communication of the ATOS system will not be considered part of the core iDetecT4ALL communication, so MIL has no participated at the WP4 activities.

The second period begin having as starting elements

- Specifications for ATOS (Task T4.1, deliverable D4.1)
- A block diagram of the ATOS
- A list of possible to use components and providers;
- Specifications for the ATOS command and control block;

The main objectives of the period were:

1. Provisioning with necessary components: All the necessary components were bought. A long period was necessary to obtain the thermal image sensor
2. Testing the components: The thermal camera integration from a thermal image sensor and a IR lens
3. Design and manufacturing of the electronic board of the control and command block were designed and tested two versions of the electronic boards. The third is coming.

In this period were achieved:

- A thermal camera with specific performances was developed using a thermal image sensor and a IR lens;
- A command block ensuring the modularity of the system was designed , manufactured, tested and improved;
- A Command Protocol document was elaborated and tested;
- Software components were elaborated and used to test the system. One of them became part of the iDetecT4All software (T6.3 Software Development and Integration)
- A converter RS232 – RS422 was designed , manufactured and tested;
- A dedicated power supply was designed, manufactured and tested;
- The functionality of the ATOS and additional components was tested and demonstrated.

The ATOS was successfully tested as a component of iDetecT4ALL.

There are not major deviations from the DoW except the time schedule.

All the WP4 objectives were achieved and no impact on others tasks or resources were generated.

ATOS was tested successfully as part of the iDetecT4ALL system

A request for a model utility patent was submitted

A web page on Pro Optica web site regarding participation in iDetecT4ALL

WP5

The objectives of WP5 were:

Design and Deliver the IDetecT4ALL Communication: Communication Controller Unit (CCU) and Master Communication Controller Unit(MCCU) including internal and external interfaces.

All objectives were achieved and successfully demonstrated during multiple field trials. A part of their process in the objectives achievement the following main activities were executed: **T5.1** - Communication system functional requirements were defined based on the use cases and scenarios defined in WP1 Technology Architecture and Field Trial Prototype defined in WP2. Communication system architecture including detailed block diagrams and interfaces was defined together with detailed interface definitions with the iDetecT sensor unit and detailed protocols between MCCU and the control centre. Seven major use cases (from communication infrastructure perspective) were indentified and documented. A part of **T5.2** hardware and software design of the Communication Controller Units were executed and integration tests with specially developed ID2 sensor and back-office simulators were carried out as part of **T5.3** to assure that the communication system operates as expected. Multiple Communication System Functionality & Performance Testing including solution optimization were executed as part of **T5.4.** Based on results of the lab testing and the integration phase, the final prototypes were manufactured and delivered to the field tests sites as part of **T5.5**.

All WP5 deliverables submitted and milestones were achieved. Multiple Field Trials in Israel, Portugal and Belgium demonstrated high performance and full matching of expected functionality during different configurations and weather conditions.

The only deviation from the original schedule was two month delay in submitting of D5.3 and this is due to overall project delay and the need to integrate with additional ID2 sensor communication simulator provided by partner IPL.

WP6

The objectives of WP6 were:

a) To develop an integration plan.

b) To develop System Level technological components needed to complete and enable integration of the various Technological Modules developed by WP3, WP4, and WP5 to meet the WP1 End User requirements and to enable “end to end” Field Trial Prototype.

c) Provisioning of the Field Trial Prototype by integration of the above developed modules and prototype units of Sensors, Tags, Alert Tracking Observation and Communication.

d) Test the functionality of the system in laboratory environment and ensure its readiness for field trials.

e) Carry a Test Readiness Review to ensure successful interfacing with the follow on WP7 and WP8 Field Trials.

All of the work package objectives were met while keeping the schedule presented in the DoW.

Integration plan was included in D6.1.

All technological subsystems were developed. Due to some difficulties and delay in the sensor's development and in order to compensate on the loose of time the technological partner have also developed communication simulators and hence the integration could started before the end of the development of the sensors.

System Field Trial Prototype was presented and tested in 2 internal sessions and field trials prior to the formal field trials.

The system was fully and successfully tested.

Test Readiness Review was conducted with the participation of all partners in Israel.

The extensive and rigorous preparation led to smooth final trials.

Figure 4 – Full integration of the System Prototype at IPL, Broadstairs, UK

Figure 5 – Field Trial Prototype in field testing

WP7

The current WP was dedicated to the validation and testing of the prototype system in facilities located in the International Airport of Faro (Portugal). The original DoW stated that the field trials would take place in Thessaloniki. Nevertheless extensive site survey in all locations (Thessaloniki, Liege and Faro International Airports) made clear that Faro Airport has a number of advantages that could prove vital for a successful implementation of the Field Operational Trial (FOT). While a second field trials session will take place in Liege.

Field trials included measurements regarding:

- Performance envelope - The overall detection capabilities of the system
- Positive detection probability - False negative rate
- False alarm rates - False positive rate

The current WP7 was led by 3DSA but almost all partners were involved in it:

- End Users: update requirements and scenarios stated in WP1 and report on the findings Technology Partners

- Technology Partners: Install and adapt the system to the test requirements, train and support the end users during field trials

T7.1 Test plan and logistic requirements

D7.1 was submitted in the previous period, but was required for re-modification by the iDetecT4ALL project reviewers; Therefore, D7.1 resubmitted at February 2011. AIL coordinated the process of modification of the document and integration of the outcomes and conclusions of sequential evaluation process executed of three events that accorded during this period:

1) In the 5th project meeting in FARO airport (March 2010) in which the project status and the technical delays where discussed and a 6 month project extension (M30-36) was requested
2) The Lab tests run by IPL and the technical requirements for modification of tests process as stated in old D7.1
3) In the 7th project meeting in Israel and the following system integration (WP6) that set the finale requirements for the field trials tests

Based on the above evaluation and coordination process, the successful collaboration between 3D and AIL enabled modification and resubmission of document D7.1, that was finally approved by the reviewers. Revised test plan was prepared by IPL with 3 use cases and a number of scenarios triggered by specific events.

The unfeasible value of the large quantity of tests were highlighted and accurate probability estimates (e.g false alarm rates) can only be measured in tightly controlled laboratory conditions rather than in an uncontrolled environment such as the field trials. To produce these types of results will require a large quantity of test data which is outside of the WP7 scope (Faro and Liege). To ensure orderly execution of the field trials related to sensor performance, IPL prepared scripted storyboards describing the sequences of activities required to implement test cases in the revised test plan.

T7.2 Field trial prototype systems installation training and integration

The purpose of this task is to present the results and conclusions derived from the Field Trials that took place in Faro Airport as described in the previous deliverable: D7.1 – Test Plan and Specifications.

During the system operation the consortium did not face any particular problems or any significant issues. All field trial objectives were met and everything went according to plan. Due to the changeable weather, we were able to test in the rain and sunshine, day and night and moreover we were able to undertake additional testing to test the system further.

T7.3 Field trials implementation and reporting

This task was dedicated to the trial and validation of the iDetecT4ALL prototypes. The trial was executed according to the test plan implemented in Task 7.1, where participating end-users will test the system's ability to detect intrusions into the restricted area and recognize the authorized entrants. The unauthorized intruders were identified in several testing areas. FOT activities monitor, analyze and evaluate the findings of the "multi phased" tests in order to quantify the performance and the proof of concept of iDetecT4ALL system against the set of measurable success criteria parameters already defined in WP2 followed by the indoor laboratory test results of the sensor and the ID tag as made in WP3 and the outdoor laboratory test results of the iDetecT4ALL system integration.

The operational activities were dedicated to the overall management operations of the laboratory tests, the outdoor tests and the FOT along with the PCD included the following actions:

- Administrative and coordination - assistance of the monitoring activities at the sites of the test (IPL, AZI and at the selected end user locations).

- Review of the test deployment plan, training schedule and reporting tools at the laboratory, outdoor, FOT and PCD

- Data capture activities

- Management of the corrective action

3D and AIL monitored performance, provided support and instructions to the tests' participants and produced the final report on the result of the field trials. All technical partners participated in the field trials.

Overall, the field trials were very successful and over 1447 intrusion events were detected with virtually no false detections. The system was consistent in finding friend and foe. All the scenarios and test cases that were described in the Field Trial Plan were implemented, allowing the collection of over 100Gb of sensor log data.

During the system operation the consortium did not face any particular problems or any significant issues. All field trial objectives were met and everything went according to plan. Due to the changeable weather, we were able to test in the rain and sunshine, day and night and moreover we were able to undertake additional testing to test the system further.

The actual trials took place in February (14-18/2) and the statistical analysis of the data gathered tool place in March and April. Results were very positive for the system and the consortium is positive that there is a good market opportunity to materialize and exploit the knowhow gained in the project in a number of products.

WP8

This WP is dedicated to the final Field Operational Trials of the IDetecT4ALL prototype system that took place in LACHS Storage Warehouse (LSW) located at LACHS cargo facility located in the International Airport of Liege (Belgium). The following infrastructure sites were available in Liege Airport for the presentation and proof of concept demonstration of the prototype system:

- Scenario D **–** Indoor Cargo Storage, Provide coverage of enclosed air cargo pallets that are located within an indoor cargo storage facility

- Scenario E **–** Outdoor Cargo Storage, Provide coverage of enclosed air cargo pallets at a temporary outdoor storage location within an airport restricted area.

For the above mentioned use cases, a number of operational cases were demonstrated:

- Restricted cargo warehouse

- Outdoor storage of clear to fly cargo pallets

The trial was completed as expected although some temporary difficulties were faced with intermittent communications issues. This was due to a high level of wireless traffic using the same channel as the remote sensor communications. A separate network channel was installed to overcome the problem and the system demonstration was successful.

The complete functionality of the system was demonstrated to the Project Officer and Reviewers, and a high detection rate was experienced. The only system performance issue noted was that on a small number of occasions ‘friend’ was detected as ‘foe’. This is attributed to the tag emitters (On a loose fitting tabard tag vest) being hidden from the sensor. This is not considered a major issue, as all the intrusions are detected.

The following are Proof of Concept Demonstration (PCD) significant results:

- System coverage - The detection rate of penetration attempts was excellent. Over 377 intrusions were detected.

- Ability to Handle High Bandwidth Traffic - The iDetect4All system communication topology and protocols has been robustly designed and no drops of packages were identified.

- Ability to Correlate Events - The iDetect4All consortium was aware for this challenge and took the following measures:

    1. The communication protocols were changed. Each reporting message is including a unique identifier, based on time.

    2. As part of the system setup, the iDetect4ALL system has synchronized clocks between the sensors and the Command and Control server.

    3. As part of the system robustness, the communication regimes between all subsystems has forced the ACK (acknowledge) feedback for each message.

- As a result, correlating events become easy and seamless.

- Ability to Identify a Penetration Attempt - Detailed forms was prepared and the data collection was done according to them. As a result identifying the penetration attempts was fully recorder.

- On the technical level each sensor has 16 detectors with sample rate of 10 Hz which has created a very redundant system.

WP8 was led by LACHS with all partners' involvements:

- Due to personnel changes in LACHS who originally was supposed to provide this deliverable, AIL has provided assistance in the production of the deliverable.

- End Users: update requirements for the predefined Use Cases and review the scenarios already defined in WP1 (D1.1 and D1.2) and evaluate and reported on the findings of the trials of WP3, WP6 and WP7, and based on the agreed evaluation methodology (D9.1)

- Technology Partners: Install and adapt the system to the test requirements, train and support the end users during field trials (as defined in WP6)

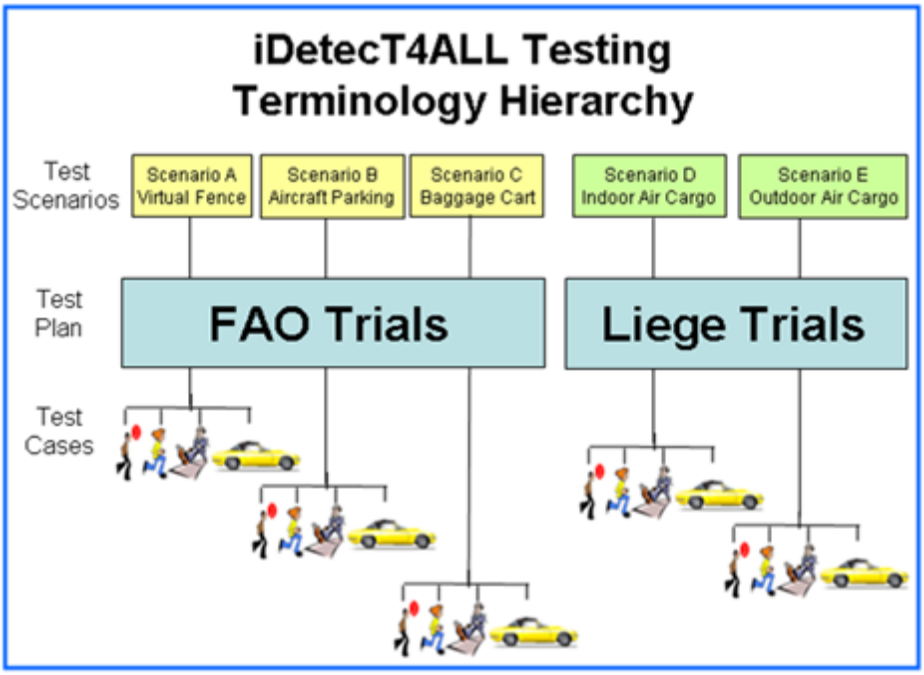
The actual trials took place in March (21-24/3) and the statistical analysis of the data gathered tool place in April and May. Results were very positive for the system and the consortium is positive that there is a good market opportunity to materialize and exploit the knowhow gained in the project in a number of products.

WP9

WP9 was dedicated to the evaluation and analysis process of the iDetecT4LL system testing and the field trials results as captured and collected during the execution of the FOT (Field Operation Trails) at FARO International airport (Portugal) as defined in WP7, and during the execution of the PCD (Proof of Concept Demonstration) at LSW (LACHS Storage Warehouse) located in Liege international airport (Belgium) as defined in WP8, The overall evaluation and analysis process of the iDetecT4LL system testing and the field trails results was required the involvement and contribution of all consortium partners.

The results were compared against the set of measurable success criteria parameters already defined in WP2 followed by the laboratory test-results of the sensor and the ID tag as made in WP3 and the laboratory test-results of the iDetecT4ALL system integration.

The Field Operational Trials (FOT) and the Proof of Concept Demonstration (PCD) of the iDetecT4ALL system were conducted at two end-users' location FAO international airport and LSW at Liege International airport and demonstrated by the following chart:



The system performed well with no missed detections. At all times, penetrations were identified and flagged through the system to the back office, demonstrating a detection rate of 100%.

There were some detection events which incorrectly identified foes instead of friends. This may have been due to the friend's emitters being shielded from the sensor's receiver, however, in this case detection would have alerted the user to investigate and find that a friend had triggered the system.

Integration between all the subsystems worked smoothly.

The overall performance of the iDetect4All system and the solution could be considered as reliable and seamless.

1.4 The potential impact

The iDetecT4ALL project consortium was originally assembled from 4 end users partners out of the 10 partners in the project. These partners have provided throughout the project their input and their requirements have been taken into account during the development process. This was done in order to ensure a result well in line with the requirements from the future users of the product, and has proven very valuable for the project.

1.4.1 Competiveness

iDetect4ALL allows both detection and authentication of objects through the use of a single sensor, optimising the performance and reliability of the system. iDetect4ALL overcomes the limited sensing capabilities as well as the very high costs of existing security equipment, eliminating the barrier to make effective intruder detection security widely available for all types of critical infrastructures (CIs), especially those with budget constraints.

Competition and complementary product providers are key players which can influence iDetecT4ALL‘s technological and business development. These are thoroughly analysed on iDetecT4ALL‘s Security Industry Survey Report.

Competition:

- Direct Competition (existence of rival products or services within the same market).
- Indirect Competition: A product that is in a different category altogether but which is seen as an alternative purchase choice; for example, coffee and mineral water is indirect competitors.

Complementary:

- Maximum effectiveness: combination of technologies to deter, detect, frustrate... (e.g. fencing only deters). Holistic approach (never a single system in isolation. e.g. radar activated surveillance). But a single interface.
- Paradigm change: layered perimeter security from the outside in. Flexible.
- Planning and integration for maximum effectiveness and operational efficiency.
- Complementary systems (inc. fence sensor systems).
- Use open protocols to interface with other systems (such as CCTV, Google Earth positioning).
- Integrate with management systems (—this person has been coming in and out of the CPD too many times today).

A preliminary identification of the physical intrusion detection (PID) market offer emphasised the need to develop a dual vision of the competitors. Indeed, the current products dedicated to intrusion detection may interact with iDetecT4ALL‘s novel solution in two ways: compete and/or complement.

Competitive Intruder Detection Technology Types have been identified as follow:

- **Detection systems** are designed to alert when a non-authorised intrusion occurs. They used to be implemented in concurrence with intrusion deterrence systems. There is a wide panel of them and the most natural classification to be made relies on the physical property they use.
- **Tracking systems** refers to systems (device/software) aimed at real-time following of the progression of an intruder within the guarded perimeter. Relevant technologies in this field are video analytics and radar/laser scanning.
- **Recognition systems** are AI-based detection systems which are programmed to detect specific patterns. The most widespread recognition systems are video analytics.

- **Identification systems** use biometrics to determine the identity of the intruder. State-of-the-art in this field is long range facial recognition.

None of these products alone would be a competitor to the whole offer of iDetecT4ALL solution: a single product would not realise an intrusion detection purpose efficiently, whereas a combination of them would. Some competitors provide all-integrated solutions more or less equivalent to iDetecT4ALL's: they are iDetecT4ALL's competition core. These companies will be identified, benchmarked and integrated in the business model development.

Two types of competition can be laid stress on:

- Direct Competition: Existence of rival products or services within the same market.
- Indirect Competition: A product that is in a different category altogether but which is seen as an alternative purchase choice.

Competition and complementary product providers are key players which can influence iDetecT4ALL's technological and business development in a direct or indirect way and stems from the evaluation of the competition and complementary product providers listed below.

Although many competitors have been listed, few could really steal market shares from iDetecT4ALL: few focuses on intruder detection to a similar extent.

iDetecT4ALL presumes to be the best innovative and cost effective solution on the security market, which gives it a serious competitive advantage. Nevertheless this assertion has to rely on a solid market analysis, so that iDetecT4ALL characteristics can be visible among the wide security offer.

Both types of competitors have been identified and benchmarked. This provides us with useful information on competitor's offers, such as prices, reliability, relevance, quality standards, etc. This information is of great importance when it comes to determine some of iDetecT4ALL_s commercial parameters. It will be possible to adjust its financial degrees of freedom to meet its goal.

1.4.2 Ethical issues – data protection and dual use

The iDetecT4ALL technology's main application is the identification of optical tags which may be carried by personnel as part of the security regulations. Potential ethical issues related to the testing and use of these tags were identified in the project proposal, and described together with the suggested procedures for dealing with them. During the field trials carried out within the project, when the iDetecT4ALL system was tested by volunteering individuals, the suggested procedures were followed as needed and no ethical conflicts were observed.

At the trials volunteers amongst the staff members of the partner organizations were recruited, and during the course of the tests these volunteers wore the identification tags. The tags allowed monitoring of the movements of the volunteers within specified zones, where the sensors were located inside the facility. The iDetecT4ALL project proposal mentions that the testing would be associated with the informed consent of the participants. The procedures for obtaining the consent as well as additional privacy issues were laid out, and these are the procedures followed at the time of the field trials, as described here below:

Informed consent

All participants to the field trial were volunteers from within the project partner organizations, and each one was assured competent to give voluntary informed consent and able to freely understand and ask questions. A detailed presentation of the technology and the field test operation was given to the volunteers prior the actual testing, as part of the training and preparation actions. In the end of the training, participants were given a consent form stating their willingness to participate to the trial and their understanding of the operations. Explicit consent was obtained from all participants, and any participant was able to withdraw from the testing team at any given time, without any implications.

The volunteers wore ID tags allowing the monitoring their movements within specified zones. The tags were required only for the specific scenarios tested and the volunteers wore them only during the test hours. A Tag was issued to the participants in the beginning of the test hours and handed back and stored in a secure

place just after the test hours. Any concern regarding unauthorized monitoring during working hours was therefore eliminated.

A list of participant names was not necessary as people were identified only by a random number ID tag which was given anonymously. No other data was held.

Privacy

During the field trials there was no need for personal data to be collected. The prototype system only detects the presence of a unanimous intruders or tags, carried by test participants, in the restricted areas within the test site. The prototype will detect whether the tag has an access right or not, and will indicate if an intruder entered the protected zone, with no need to record or identify the specific individual.

Since the prototype system only detects the presence of a tag, without recording or identifying the individual carrying it, it was not necessary to apply to any DATA PROTECTION AGENCY for approval. Nevertheless, ANA informed officially all authorities and stakeholders in FARO airport about the field trials.

Tracking the location of people

The IDetecT4ALL system detects the presence of objects (human beings, vehicles, goods), inside or in the surrounding of restricted critical infrastructures. The system can identify authorized objects and will alert if an unauthorized objects are found within the protected zone.

To validate the technology tracking the location of people was executed according to the following rules:

- Only people participating in the field trial were tracked, meaning they had signed an informed consent form.
- The participants were identified only by a random number ID tag which was given anonymously; no personal data was collected or stored.

Review recommendations

During the two periodic reviews carried out within the iDetecT4ALL project several comments regarding ethical issues and suggestions for improvements were included in the review reports. The project consortium took these comments into account for the implementation of changes in order to fulfill the ethical requirements:

- It was agreed that a dedicated Dual Use Advisory Board, planned in the original project proposal, was not necessary, but an Ethical Advisory Board was activated during period 2. The board was present at the field trial in Liege where it presented "Ethics Advisory Board report" produced in January 2011 (further described below.
- General recommendations based on the Spanish and UK laws on data protection were included in *deliverable 10.4.*
- Informed Consent forms were signed by members of the consortium who participated in the trials both in Faro and Liege.
- Privacy by design has been deliberately not implemented at this stage and deferred to eventual deployment of commercial solutions that will take into account local legal requirements.

1.4.3 Socio-economic impact and the wider societal implications

When initiating the iDetecT4ALL project the consortium have set up the following socio economic goals:

1. To create one technology for both intruder detection sensors and remote optical ID tag reading
2. To create one technological solution applicable for all critical infra structures with restricted areas.
3. CAPEX – a magnitude of order reduction in the costs of equipment per protected area
4. OPEX dramatic reduction in the operating expenditure due to:
    a. Much lower false alarm rates
    b. Much less energy consumption – due to efficient use of energy radiated for detection
5. Deployment - dramatic reduction in the costs of installation
6. Dimensions - significant reduction in the size and volume of the sensing units

The iDetecT4ALL system presents one technological solution which includes both intruder detection sensors and remote optical ID tag reading. Through integration sessions and field trials the iDetecT4ALL system has proven successful in the following areas:

- protection of aircraft and baggage as an ad hoc perimeter
- fixed area perimeter protection

- gate security
- deployment to secure an incident

It is further easy to extend the concept to general incident management, such as required around a chemical spill or crime scene.

The solution offered by the iDetecT4ALL system can be tailored to each client in order to fit their requirement of the specific infra structure, while using the client's existing equipment. The information system integration experience and holistic approach enables a turnkey offering of integrated products depending upon client needs, as well as truly open standards enabling seamless integration into any existing security system solution. The efficiency of the iDetecT4ALL system will thereby reduce the costs of equipment per protected area.

The iDetecT4ALL system is characterized by low maintenance and a low power consumption, which allows us to see a dramatic reduction in the operating expenditure. The sensor system has further proven to be quick and easy to deploy; it can be mounted in a vehicle and driven to a location that requires an ad hoc protection, or for less urgent situations it can be deployed manually

Figure 6 – Sensors

The prototype development of the sensor partially used off-the-shelf products to keep costs down and maintain schedules. For a production unit we would expect to condense the construction to two small PCBs, and eventually down to one, with market demands dictating the further ASIC development.

Figure 7 – Sensor's inside

1.4.4 Dissemination & Exploitation in iDetecT4ALL

T10.1 Public Website (EVR)

Constantly update of the Website:

- News & Events, Home, Publications, Related Projects, Links & Legal Notice.

T10.2 Dissemination and Exploitation plan (EVR + ALL)

The dissemination and exploitation document enclosed a plan for the implementation of information dissemination actions. Define the targets and the activities to be carried out together with their timing and implementation details.

It also define the industry conferences, fairs and forums that should be targeted by the partners in order to ensure as wide as possible take up of iDetecT4ALL research.

Activities carried out:

- Follow up of the planning established on the Dissemination & Exploitation.
- Updated version of the Dissemination & Exploitation Plan & Pipeline.
    - Constant Update of the Dissemination Pipeline

T10.3 Information dissemination (EVR, MIL, CU, AIL)

These activities cover:

- The preparation of dissemination material explaining the basics, the research orientations and the potential impact iDetecT4ALL.
- Relevant dissemination material developed

iDetecT project presentation (flash)
iDetecT Brochure (Spanish)
iDetecT Brochure
iDetecT project poster
iDetecT Field Trial Poster
iDetecT project & Faro tests video
Liege Field Trial Poster
Liege Field Trial Folder
Liege Field Trial pen drives
Liege Field Trial pens

- Maintenance of a public website.
- Participation to Exhibitions, conferences and trade shows in Europe selected.
    - Attending to SRC10 Conference September 22nd - 24th 2010, Ostend, Belgium, in order to do an informal dissemination of the project and in order to analyze the market and other related projects for the business plan.
    - Attending to HOMESEC 2011 Homeland Security Fair March 15th – 18th , 2011 - Madrid, Spain
        - Participation with a stand where the project was presented to the audience. Poster was showed: project story, goals achieved and Faro tests results. A formal and informal dissemination of the project was done on this event.
- Participation on iDetecT4ALL Field Trail – Liege (Brussels). March 21-24, 2011
    - Field Trail invitation, folders, pens and pen drives
    - Marketing pictures

T10.4 Business Model and Commercial evaluation

This task includes the commercial evaluation of the iDetecT4ALL service and the planning of iDetecT4ALL roadmap to be undertaken after and beyond the project's successful termination

Development of a business model for iDetecT4ALL selected product and services

Following analysis of the industry survey, the demand acceptance study, and other relevant internal and external information collected, the objective of the commercial evaluation will be to design the most appropriate and effective business model for the iDetecT 4ALL system.

- Exploitation pipeline. This tool (excel based), identifies' potential clients, Competition and complementary product providers operating in Europe, Emergency Product Resellers, First Responders Organizations, CIP Researcher, Academic and Industry Expert Market which can be of interest to the consortium.
- Main and strategy objectives of iDetecT4ALL.
- Identification of key trends and challenges that characterize iDetecT4All's market
- Product development.
- Market Analysis
    - Market Forecast
    - Emergency response Authorities.
    - Competition and Complementary Product Providers.
    - Emergency Product Resellers.
    - CIP Researchers, Academics and Industry Experts.
    - Manufacturing partners.
- Commercial Strategy and Implementation
    - Competitive edge
    - Marketing and Sales strategy.
    - Services operation plan.
    - User data protection.
- Financial Plan. An excel document where is described a proposal where a detailed commercial strategy for the next five years.

  Herein will be find exhaustive an detailed information regarding potential clients infrastructures, potential market growth, potential scenarios, forecasts, price product and solution definition, incomes forecast, theoretical resellers activity, expenses, potential iDetecT4ALL offices, HHRR data, funding and investment data, P&L, etc.

1.4.4.1 Dissemination activities

A project start, a dissemination plan was set up by the consortium and contained a planning of information dissemination actions to be carried out in the course of the project. The present section provides a summary of the main dissemination activities carried out within the project, in accordance with the original plan set out.

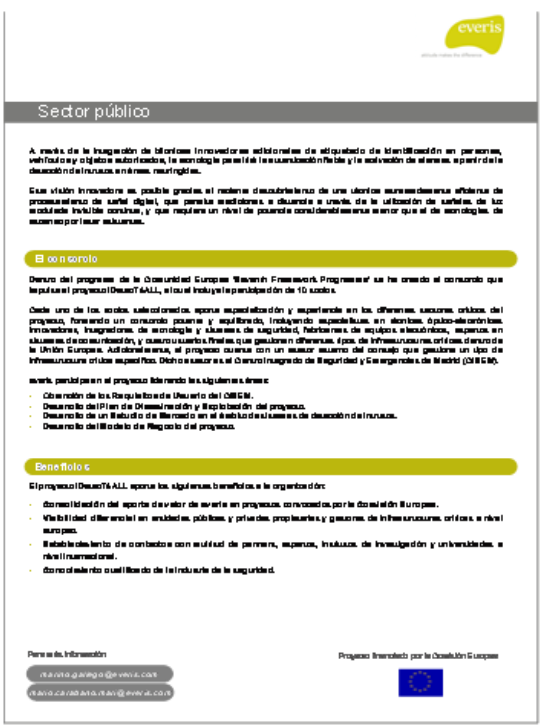
<table>
<tr><th>Specific Activity</th><th>Objectives</th><th>Target Audience</th><th>Channels</th><th>Results</th></tr>
<tr><td>PSCE Forum</td><td>• To build awareness of the project.</td><td>General audience attending Forum. Primary groups of interest</td><td>• Informal face to face and small meeting</td><td rowspan="7">Effective communication of the project.
• Establish contact with related projects
• Communication of finding results among stakeholders

Stimulate ongoing interest in the work of the project.</td></tr>
<tr><td>SRC10 Conference in Ostend, Belgium, 22-24 September 2010</td><td>• To communicate research findings to stimulate ongoing interest in the work of the project.</td><td rowspan="4">Audience attending Events. Primary groups of interest</td><td>• Formal face to face
• Informal Face to Face
• Poster Session presentation</td></tr>
<tr><td>HOMESEC 2011, Homeland Security Fair March 15th – 18th , 2011 - Madrid, Spain</td><td>• To maximize exploitation opportunities.</td><td>• Stand
• Formal face to face
• Informal Face to Face
• Poster Session presentation</td></tr>
<tr><td>SRC09 Conference in Stockholm 29-30 September 2009</td><td>• To lay the groundwork to establish and reinforce a wide network of potential customers.</td><td>• Formal face to face

• Informal Face to Face</td></tr>
<tr><td>SRC10 Conference in Ostend, Belgium, 22-24 September 2010</td><td rowspan="2">• To communicate research findings to stimulate ongoing interest in the work of the project.</td></tr>
<tr><td>Non-scientific publication: Innovation in critical Infrastructures” ESP</td><td>General website visitors. (Stakeholders)</td><td>• Web site</td><td>• Pending Publication</td></tr>
</table>

1.4.4.2 iDetecT4ALL dissemination material

Figure 8 - Project brochure (Spanish)



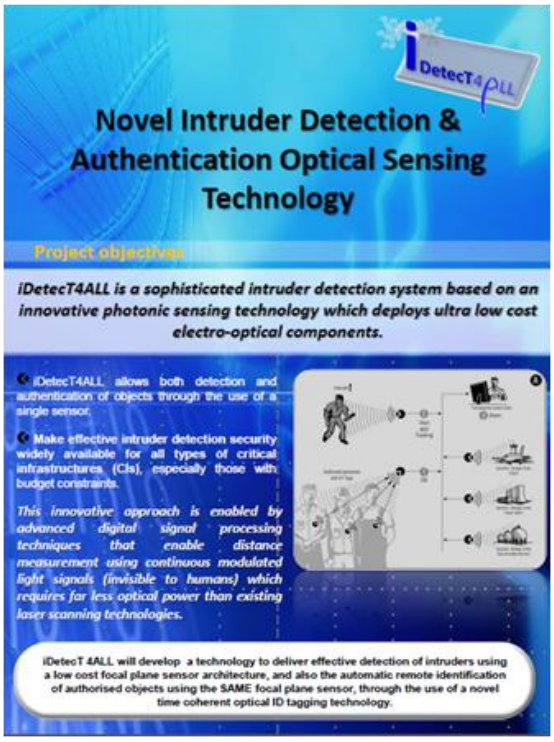


Figure 9 - iDetecT4ALL project poster & Field trial poster

Figure 10 - iDetecT4ALL Liege Field Trials folder

Figure 11 - iDetecT4ALL pen drives & pens for the Field Trial event

- 40 pen drives of 2GB for the stakeholders attended to the Field trail, with information about the project.
- 100 iDtecT4ALL pens for the stakeholders attended.

Figure 8 - iDetecT4ALL Field Trials video

A video was developed in order to show the iDetecT4ALL solution and what has been done along the tests carried out at Faro (Portugal).

1.5 Public project website - www.idetect4all.com

iDetecT4ALL's website is one of the most important channels chosen to achieve potential clients. From web site clients will be able to be informed about latest news related to the project.

Main objective of iDetecT4ALL's web site is to build awareness at a relatively big scale and to inform about the project's news to primary and/or secondary and/or tertiary groups of interest.

Website constitutes one of the main communication channels within the project's Dissemination and Exploitation Plan. It provides complete external visibility as it contains general information on project goals, scope, focus and work progress, as well as on consortium partners.

A SEO (Search Engine Optimization) tries to increase the visibility of a website on the Internet, and also encircles tasks related with website promotion which have a direct impact on the website's frequenting. Website can works also as a proactive mechanism where partners will be able to reach feedback from.

Furthermore others sections are attached in the web:

- **HOME:** Project information is provided, such as project history, description and objectives of the project, project coordinator and further information of 7th Framework Programme.

Figure 9 – iDetecT4ALL website

- **News & Events:** This page provides information on coming project events as well as industrial events relevant for the consortium to attend. Any piece of news related to the iDetecT4ALL project is published there.

  The latest news & events are also displayed in the home page's scrolling box.

  Additionally, the web includes an RSS feed which enables interested parties to view iDetecT4ALL's news & events as they are published.

- **Partners:** This section provides information about consortium partners, the tasks each one handles within the project's development and their contact details. The link redirects to the corporate website of the corresponding organisation.

- **Product publications:** This page provides information on the results of development work being carried out during the project. The technical details on the product are presented. The information will be permanently updated throughout the project.

  These publications might be articles, academic papers, presentations made during conferences, exhibitions, etc. Promotional materials are also located in this section. Clicking on the link opens a new tab displaying the material.

- **Related projects and links:** This section provides basic information and links to other projects - EU-funded or not - currently being executed in Europe and somehow related to the topics of iDetecT4ALL. There are two types of projects related to iDetecT4ALL:

- **Contact:** This section provides contact details of the official focal point for the project. The contact details of the Project Coordinator and the Project Officer are published, as well as the contact details of the partner responsible for administrative & financial management.

Coordinator:

iDetecT4ALL coordinator is Instro Precision Limited. Founded in 1960, Instro Precision Limited is one of the leading suppliers of sensors and sensors support solutions for target acquisition and surveillance systems in the World. It has achieved this position through a constant drive for innovation and establishing an excellent reputation working with major homeland security and defence equipment prime contractors.

Instro's experience includes participation in many complex long range surveillance system development projects including the design of high performance multi-spectral sensor systems for homeland security and border protection.

Instro's capabilities include electro-optical research, design, development and manufacture. Of particular relevance to this FP07 project are the company's new range of laser diode rangefinders, which were developed entirely in house using new technology researched and patented by Instro, and which offer class leading operating range, beam divergence and measurement precision. It is this technology that has the unique potential to provide low cost, focal plane array based intruder and Automotive collision warning sensors.

Contact:

Project coordinator:

Mike Casey

Electro-optic Project Manager

Instro Precision Ltd.

tel +44 (0) 1843 60 44 55

E-mail: mikecasey@instro.com

Website: www.instro.com

Project management:

Moran Naor

Project Manager

Tel. +972 3 373 2010

E-mail: naor@arttic.com

Website: www.arttic.com

Commission Project Officer:

Project Officer: Dr. Massimo CISCATO

Tel: +32-2 299 15 50

Fax: +32-2 298 80 22

E-mail: Massimo.CISCATO@ec.europa.eu

2. Use and dissemination of foreground

2.1 Section A

During the iDetect4ALL project no per reviewed publications were made.

LIST OF DISSEMINATION ACTIVITIES

NO.	Type of activities	Main leader	Title	Date	Place	Type of audience	Size of audience	Countries addressed
1	*Conference*	EVR	Counter Terror Expo 2009	07 July 2009	London	Security Professionals and Stakeholders	> 500	European wide
2	*Conference*	EVR	SRC09	29-30 September 2009	Stockholm	Security Professionals and Stakeholders	> 500	European wide
3	*Conference*	EVR	*SRC10*	22nd - 24th September 2010	Ostend	Poster Session	> 500	European wide
4	*Conference*	EVR	*HOMESEC11*	15th – 18th January 2011	Madrid	Stand	> 500	European wide

2.2 Section B

Part B1

LIST OF APPLICATIONS FOR PATENTS, TRADEMARKS, REGISTERED DESIGNS, ETC.					
Type of IP Rights: Patents, Trademarks, Registered designs, Utility models, Others.	**Confidential**	**Foreseen embargo date**	**Application reference(s) (e.g. EP123456)**	**Subject or title of application**	**Applicant (s) (as on the application)**
Utility models	Yes	02/March/2017	U00004/2011	Smart multi sensor	PRO-OPTICA

Part B2

There were no exploitation activities in project iDetecT4ALL

#	Type of Exploitable Foreground[3]	Description of exploitable foreground	Confidential YES/NO	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application[4]	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved

Exploitation Result N°1 -

Its purpose	
How the foreground might be exploited, when and by whom	
IPR exploitable measures taken or intended	
Further research necessary, if any	
Potential/expected impact (quantify where possible)	

[19] A drop down list allows choosing the type of foreground: General advancement of knowledge, Commercial exploitation of R&D results, Exploitation of R&D results via standards, exploitation of results through EU policies, exploitation of results through (social) innovation.

[4] A drop down list allows choosing the type sector (NACE nomenclature) : http://ec.europa.eu/competition/mergers/cases/index/nace_all.html

3. Report on societal implications

The questionnaire was filled in the SESAME