European Commission

Security Research Projects
under the 7th Framework Programme for Research

EU Research for a Secure Society

April 2016

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2016

ISBN 978-92-79-56875-6
doi:10.2837/796260

Cover picture: © Fotolia/Shutterstock

Printed in France

Printed on a CONDAT silk paper, certified by the PEFC™ and ECF

INTRODUCTION

Investing in security research for the benefit of European citizens, critical infrastructures, SMEs and industry

> *"Under its wider R&D budget for 2007-2013 – known as the Seventh Framework Programme for Research (FP7) – the EU is investing EUR 1.4 billion in security research. This catalogue presents an exhaustive overview of all projects currently supported by FP7's Security Research budget as of December 2013."*

Europe has never been so peacefully consolidated or prosperous, yet it is also vulnerable to threats such as terrorism, organised crime and natural disasters. Making Europe more secure and resilient for its citizens and critical infrastructures, while strengthening its SMEs and industrial competitiveness, is the goal of Security Research. To date, a significant proportion of the committed budget (> 22%) is going to SMEs. By stimulating research and innovation – and promoting direct cooperation between providers and end-users of security equipment, systems and knowledge – the EU can better understand and prepare itself to face risks and disruptive events in a constantly changing world.

The evolving nature of security implies many new challenges. To strengthen the respect for fundamental human rights, including privacy, research into the preparedness and response of society in the face of potential or actual threats and crises is essential. Thus, it is promising to see that European Security Research efforts in this area have increased substantially in the last few years, as readily seen in the below catalogue of FP7 projects.

These projects cover the entire range of FP7's Security theme, including advanced research into the societal dimension of security, protection of citizens against chemical, biological, radiological, nuclear and explosive (CBRNE) materials or man-made and natural events, critical infrastructure protection, crisis management capabilities, intelligent maritime and land border surveillance, pre-standardisation and the interoperability of systems.

Further information is available at:

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/industry-for-security/index_en.htm

Prepared by the European Commission, Directorate-General for Migration and Home Affairs, Unit B4 Innovation and Industry for Security, E-mail : HOME-NOTIFICATIONS-B4@ec.europa.eu "

TABLE OF CONTENTS

INTRODUCTION 1

TABLE OF CONTENTS 2

Security of the Citizens

CBRN PROTECTION

BIO-PROTECT 6
CBRNEMAP 8
COCAE 10
CREATIF 12
DECOTESSC1 14
EDEN 16
GIFT CBRN 18
ISIS 20
MODES_SNM 22
REWARD 24
SAFEWATER 26
SCINTILLA 28
SECUREAU 30
SNIFFER 32
SPICED 34
TAWARA_RTM 36
TWOBIAS 38

EXPLOSIVES

AVERT 40
BONAS 42
COMMONSENSE 44
D-BOX 46
EMPHASIS 48
ENCOUNTER 50
EXPEDIA 52
FORLAB 54
HOMER 56
HYPERION 58
LOTUS 60
OPTIX 62
PREVAIL 64
SALIANT 66
SUBCOP 68
TIRAMISU 70

INTELLIGENCE AGAINST TERRORISM

IMSK 72
RAPTOR 74
TACTICS 76
UNCOSS 78
VIRTUOSO 80

ORDINARY CRIME AND FORENSIC

AEROCEPTOR 82
EVIDENCE 84
LINKSCH 86
MEPROCS 88
MIDAS 90
ODYSSEY 92
SAVELEC 94
SMARTPRO 96

ORGANISED CRIME

CAPER 98
CONPHIRMER 100
CUSTOM 102
DIRAC 104
EKSISTENZ 106
HEMOLIA 108
SAVEMED 110
SCIIMS 112

INFORMATION GATHERING

CRIMTRACK 114
LASIE 116
VALCRI 118
ZONESEC 120

Security of infrastructures and utilities

CYBER CRIME

CAMINO 122
COCKPITCI 124
CRISALIS 126
COURAGE 128
ECOSSIAN 130
ECRIME 132
HYRIM 134
PREEMPTIVE 136
SAWSOC 138
SECCRIT 140

DESIGN, PLANNING OF BUILDINGS AND URBAN AREAS

DESURBS 142
ELASSTIC 144
HARMONISE 146
INTACT 148
RAIN 150
RIBS 152
SECUR-ED 154
SPIRIT 156
VASCO 158
VITRUV 160

ENERGY, TRANSPORT, COMMUNICATION GRIDS

AFTER 162
CARONTE 164
COPRA 166
CWIT 168
DEMASST 170
DITSEF 172
EURACOM 174
EUROSKY 176

GAMMA . . . 178
HIPOW . . . 180
INFRA . . . 182
ISTIMES . . . 184
L4S . . . 186
NI2S3 . . . 188
PANDHUB . . . 190
PANDORA . . . 192
PROGRESS . . . 194
PROTECTRAIL . . . 196
SCOUT . . . 198
SECRET . . . 200
SECTRONIC . . . 202
SEGRID . . . 204
SERON . . . 206
SESAME . . . 208
SPARKS . . . 210
STAR-TRANS . . . 212
STRUCTURES . . . 214
TASS . . . 216
XP-DITE . . . 218

SUPPLY CHAIN

CORE . . . 220
IMCOSEC . . . 222
IPATCH . . . 224
LOGSEC . . . 226
PROMERC . . . 228
SAFEPOST . . . 230

SURVEILLANCE

ADABTS . . . 232
ARENA . . . 234
ARGOS . . . 236
BASYLIS . . . 238
IDETECT 4ALL . . . 240
INDECT . . . 242
MOSAIC . . . 244
P5 . . . 246
SAMURAI . . . 248
SUBITO . . . 250

Intelligent surveillance and border security

AIR BORDERS

ARGUS 3D . . . 252

BORDER CHECKS

ABC4EU . . . 254
ACXIS . . . 256
CONSORTIS . . . 258
DOGGIES . . . 260
EFFISEC . . . 262
FASTPASS . . . 264
FIDELITY . . . 266
HANDHOLD . . . 268
INGRESS . . . 270
SNIFFER . . . 272
SNIFFLES . . . 274
SNOOPY . . . 276
TERASCREEN . . . 278

BORDER SURVEILLANCE

OPARUS . . . 280
SUNNY . . . 282

LAND BORDER

CONTAIN . . . 284
EWISA . . . 286
GLOBE . . . 288
TALOS . . . 290

SEA BORDERS

AMASS . . . 292
CASSANDRA . . . 294
CLOSEYE . . . 296
I2C . . . 298
OPERAMAR . . . 300
PERSEUS . . . 302
SEABILLA . . . 304
SUPPORT . . . 306
TRITON . . . 308
WIMAAS . . . 310

Restoring security and safety in case of crisis

CBRN RESPONSE

ANTIBOTABE . . . 312
BOOSTER . . . 314
CATO . . . 316
COUNTERFOG . . . 318
FRESP . . . 320
IF REACT . . . 322
MIRACLE . . . 324
MULTIBIODOSE . . . 326
MULTISENSE CHIP . . . 328
PRACTICE . . . 330

PREPAREDNESS, PREVENTION, MITIGATION AND PLANNING

A4A . . . 332
AF3 . . . 334
BESECU . . . 336
BRIDGE . . . 338
CASCEFF . . . 340
CAST . . . 342
CONCORDE . . . 344
COPE . . . 346
CRISCOMSCORE . . . 348
CRISIS . . . 350
CRISMA . . . 352
DRIVER . . . 354

TABLE OF CONTENTS

EMILI . . . 356
IDIRA . . . 358
IMPRESS . . . 360
INDIGO . . . 362
OPSIC . . . 364
OPTI-ALERT . . . 366
POP-ALERT . . . 368
PREDICT . . . 370
PSYCRIS . . . 372
PULSE . . . 374
SECURENV . . . 376
S-HELP . . . 378
SICMA . . . 380
SNOWBALL . . . 382
TACTIC . . . 384

RECOVERY

ACRIMAS . . . 386
CAERUS . . . 388
COBACORE . . . 390
DESTRIERO . . . 392
HELP . . . 394
RECONASS . . . 396
SAFE-COMMS . . . 398

RESPONSE

CRISYS . . . 400
DARIUS . . . 402
ELITE . . . 404
E-SPONDER . . . 406
ESS . . . 408
EVACUATE . . . 410
FASTID . . . 412
ICARUS . . . 414
INACHUS . . . 416
NMFRDISASTER . . . 418
PEP . . . 420
SGL FOR USAR . . . 422
SPARTACUS . . . 424
S(P)EEDKITS . . . 426

Security systems integration, interconnectivity and interoperability

INFORMATION MANAGEMENT

BEAT . . . 428
EPISECC . . . 430
FORTRESS . . . 432
REDIRNET . . . 434
SECINCORE . . . 436
SECTOR . . . 438
SIIP . . . 440

INTEROPERABILITY

ADVISE . . . 442
C2-SENSE . . . 444
DISASTER . . . 446
ESENET . . . 448
EUCISE 2020 . . . 450
ISITEP . . . 452
SALUS . . . 454
SAVASA . . . 456
UNSETH . . . 458

SECURE COMMUNICATIONS

EULER . . . 460
FREESIC . . . 462
GERYON . . . 464
HIT-GATE . . . 466
PPDR-TC . . . 468
SECRICOM . . . 470

STANDARDISATION

CRISP . . . 472
EQUATOX . . . 474
HECTOS . . . 476
SLAM . . . 478

Security and society

CITIZENS, MEDIA AND SECURITY

ANVIL . . . 480
ATHENA . . . 482
COSMIC . . . 484
CPSI . . . 486
EMERGENT . . . 488
IMPACT EUROPE . . . 490
ISAR+ . . . 492
PARIS . . . 494
PRIME . . . 496
RECOBIA . . . 498
RESPECT . . . 500
SAFIRE . . . 502
SLANDAIL . . . 504
SOTERIA . . . 506
SUPER . . . 508
SURVEILLE . . . 510
TRACE . . . 512

ETHICS AND JUSTICE

ADDPRIV . . . 514
ALTERNATIVE . . . 516
COREPOL . . . 518
DETECTER . . . 520
INEX . . . 522
PACT . . . 524
PRISMS . . . 526
SAPIENT . . . 528
SMART . . . 530
SURPRISE . . . 532

FORESIGHT, SCENARIOS AND SECURITY AS AN EVOLVING CONCEPT

ASSERT 534
COMPOSITE 536
DESSI 538
EPOOLICE 540
ETTIS 542
EVOCS 544
FESTOS 546
FOCUS 548
FORCE 550
FORESEC 552
SIAM 554

ORGANISATIONAL STRUCTURE AND CULTURES OF PUBLIC USERS

BESECURE 556

SECURITY ECONOMICS

EUSECON 558
SECONOMICS 560
VALUESEC 562

Security Research coordination and structuring

END USER

ARCHIMEDES 564
EU-SEC II 566
INNOSEC 568
INSEC 570

ERA-NET

THE HOUSE 572

OTHER COORDINATION

CIPRNET 574
EUROFORGEN-NOE 576
PLANTFOODSEC 578
SEREN 580
SEREN 2 582
SOURCE 584
VIDEOSENSE 586
VOX-POL 588

SMALL AND MEDIUM ENTERPRISES

3D-FORENSICS 590
GRAFFOLUTION 592
MISAFE 594
OSMOSIS 596
P-REACT 598
ROSFEN 600
SMARTPREVENT 602

STUDIES

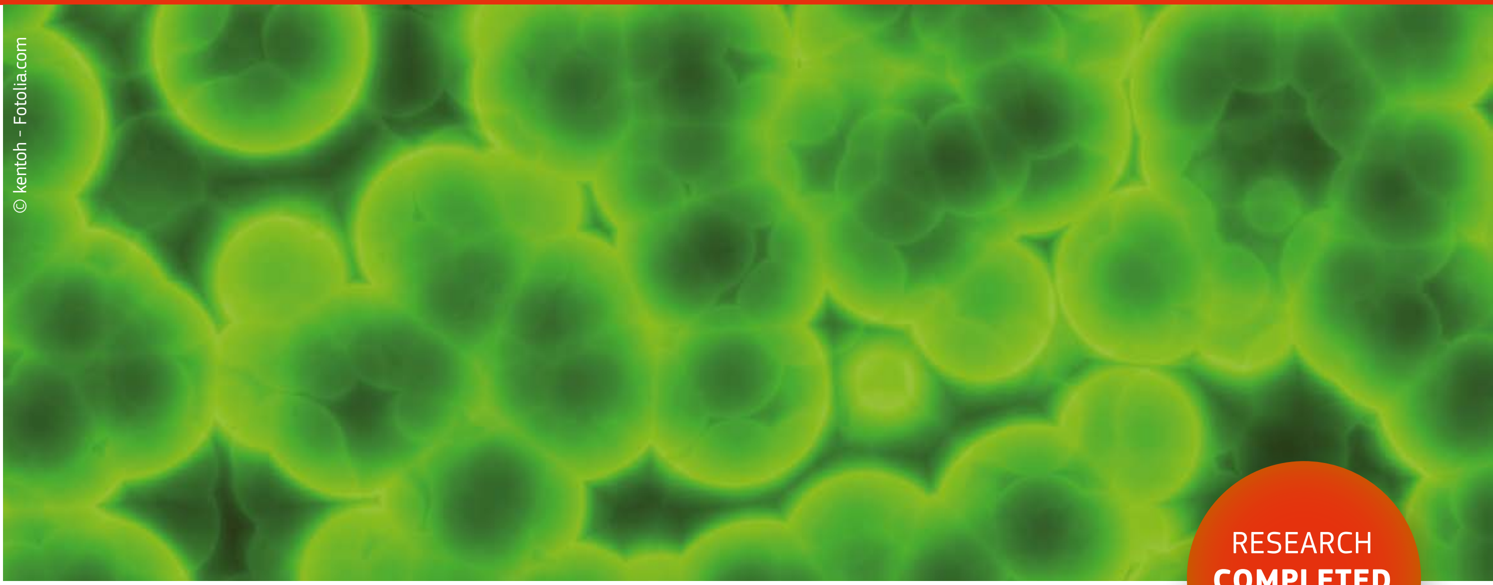
CRESCENDO 604
ESC 606
ESCORTS 608
ETCETERA 610
SECURECHAINS 612
SECUREPART 614
STRAW 616

TRAINING

DITAC 618
LEILA 620
SAFECITI 622

LIST OF PROJECTS 624

BIO-PROTECT / Ionisation-based detector of airborne bio-agents, viruses and toxins for fast-alert and identification


© kentoh - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242306
Total Cost
€3,963,556.55
EU Contribution
€3,125,577
Starting Date
01/06/2010
End Date
31/01/2014

Coordinator

LGI CONSULTING
37, Rue de la Grange
aux Belles
75010 Paris
France
Contact
Vincent Chauvet
Tel: +33 (0) 67539 8727
Fax: +33 (0) 80074 1853
E-mail: vincent.chauvet@lgi-consulting.com

Project objectives

The malevolent use of Anthrax spores on civilians in 2001 has shown the necessity to protect citizens from criminal use of biological agents. The success of such attack depends on sufficient concentration of pathogens in a defined area.

Detecting pathogenous bacteria, spores and viruses must be accomplished by triggering short-term alarm and identification of the type of threat.

Since most of the bio sensors available today are laboratory bound or require special equipment which needs training as well as experience, new systems are needed.

The concept of BIO-PROTECT was the development of a fast-alert, easy-to-use device for detection and identification of airborne bacteria, spores, viruses and toxins. It was based on bioaerosol detection by fluorescence, scattering and background aerosol measurement followed by ionisation of air flow and analysis of the spectrum of relative speed of passage, enabling identification of biological agents.

Description of the work

The work in BIO-PROTECT was structures in several technical Work Packages, addressing the following activities:

» Development of a bio-agent detection system based on a miniaturised GC-IMS (Gas Chromatograph - Ion Mobility Spectrometry) instrument able to identify and separate extremely small amounts of a wide range of organic molecules resulting from heat-decomposed organic matter;

» Integration of a particle size analyser which constantly monitors the ambient air, thus triggering a measurement if a sudden change in particle size and/or density occured;

» Improvement and integration of a continuously operating bioaerosol detector measuring fluorescence, scattering and background aerosol properties to detect presence of potentially harmful biological agents in ambient air and to trigger further identification;

» Research and development of a combined pre-concentration and pyrolysis unit for use with a GC-IMS, that can separate all types of bio-agents from aerosols. The target was to detect bio-agent concentrations likely to infect or intoxicate;

» Development of pattern analysis software for the interpretation of the acquired spectra, thereby identifying bio-agents and distinguishing them from background bacteria.

Results

The device combines the detection and identification of bio aerosols. It continuously measures the air and if a sudden change in particle amount is noticed, the particle collector is triggered. A small, precise amount of the particles is fed through an innovative sample transfer line into the pre-treatment unit, where the sample is pyrolyzed. Gases produced in pyrolysis process are fed to the GC-IMS and analysed.

Advantages for users:

- » Detection and identification with one device
- » Separation between bacteria, viruses, and toxins
- » Fast and reliable result, on which countermeasures can be initiated
- » No reagents needed, thus lower operating costs
- » Secondary sample collection available
- » Upgradable database
- » Customisable and easy-to-use web-based user interface
- » Networkability via LAN/WLAN

This device provides security personnel with a reliable tool to take fast, effective countermeasures when confronted with biological threats. Pattern analysis software has been developed for the interpretation of acquired spectra, identifying bio-agents and distinguishing them from background bacteria. Thus a database of several model-agents including bacteria, spores, toxins and viruses has been generated.

PARTNERS	**COUNTRY**
LGI Consulting	France
AVSISTA	Lithuania
C-Tech Innovation Ltd	United Kingdom
Environics Oy	Finland
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Institut für Umwelt Technologien GmbH	Germany
Robert-Koch Institut	Germany
University of Aalborg	Denmark
Environics-IUT GmbH (ENIT)	Germany

CBRNEMAP / Road-mapping Study of CBRNE Demonstrator

© Morane- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242338
Total Cost
€1,662,022
EU Contribution
€1,376,185
Starting Date
01/06/2010
End Date
30/09/2011

Coordinator

EUROPEAN CBRNE CENTER AT UMEÅ UNIVERSITY
KBC Building
90187 UMEA
Sweden
Contact
Agneta H. Plamboeck
E-mail: Agneta.Plamboeck@cbrnecenter.eu
Website:
http://www.cbrnemap.org/

Project objectives

CBRNEmap was a “phase I” Security Research project to define a strategic roadmap that will lead to a subsequent phase II, large-scale CBRNE (chemical, biological, radiological, nuclear, explosive) Demonstrator project. Its goal was to bring together end-users, industry and other stakeholders with Europe’s scientific and technical communities to address the cross-cutting activity of such a large-scale effort and to identify potential scenarios and technical solutions.

Its key objective was to evaluate the multi-dimensional challenges of countering CBRNE-based threats. Temporal events (before, during and after) were contrasted against societal targets (mass transport, public spaces, etc.) and societal sectors directly involved in such events (law enforcement, health first-responders, etc.).

These generic needs were matched by technological solutions that will be integrated at a system-of-systems level, leading to the CBRNE Demonstrator.

Results

The project narrowed down CBRNE counter-terrorism to three dimensions: the need to protect society’s vital functions, the ability to respond to CBRNE events and the need for resilience to enable society to rebuild capabilities. The generic needs of each dimension were matched with advanced technological solutions and integrated at the system-of-systems level for demonstration during phase II.

CBRNEmap’s research identified a number of gaps in CBRNE counter-terrorism and solutions to fill them. Among others, it recommends that:

» more research effort be devoted to the design of buildings and, in particular, to the design of floor plan layouts, escape routes and surface-covering materials;

» recent advances in the material sciences such as nanotechnologies argue for the development of new filters and protective equipment;

» the protection of buildings from attack require new modelling techniques to predict the spread of CBRN gas or aerosol agents;

» nano-technologies and new materials be studied for their potential decontamination applications;

» more EU research focus on the use of symbology or simplified language – including animation or other communications channels – to increase the rate, precision and absorption of public messaging about major CBRNE incidents.

Phase two of the CBRNE Demonstrator project will illustrate the usefulness of the system-of-systems approach to counter CBRNE terrorism. This will best be validated in a set of realistic scenarios where vital parameters such as successful denial of access, delay of effect, shortened time for evacuation, shortened response time, more effective health care and other considerations can be observed and quantified.

PARTNERS	**COUNTRY**
European CBRNE center at Umeå University	Sweden
Police National CBRN Centre	United Kingdom
National Institute for NBC Protection	Czech Republic
Robert Koch Institute	Germany
DGA Maîtrise NRBC	France
Lindholmen Science Park	Sweden
French High Committee for Civilian Defence	France
Compagnie Industrielle des Lasers	France
European Aeronautic and Space Company	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Foundation for Strategic Research	France
Istituto Affari Internazionali	Italy
Selex Galileo	Italy
Catholic University of Louvain	Belgium

COCAE / Cooperation across Europe for Cd(Zn)Te based security

© COCAE

RESEARCH COMPLETED

Information

Grant Agreement N°
218000
Total Cost
€2,644,416
EU Contribution
€2,031,347
Starting Date
01/10/2008
End Date
31/03/2012

Coordinator

TECHNOLOGICAL EDUCATIONAL INSTITUTE
of Halkida (TEI)
Thesi Skliro
34400 Psahna-Evia
Greece
Contact
Dr. Charalambos Lambropoulos
Tel: +30 22280 99631
Fax: +30 22280 23766
E-mail: lambrop@teihal.gr
Website: www.cocae.eu

Project objectives

Fixed and portable detectors are usually used to detect, locate and identify radioactive and nuclear material at the checkpoints such as those at road and rail boarder crossings, airports or seaports. After a first alarm signal, a secondary inspection must be performed. Handheld detectors are then used to distinguish the innocent and false alarm from the real alarms. Hundreds of innocent alarms may take place per day at the boarder control from the portal detectors.

» To make spectroscopic measurements with efficiency equivalent to that of NaI detectors and energy resolution close to that of HPGe devices but without using cryogenic systems.

» To find the direction and the distance of the radioactive source.

» To localize the source into a cargo

» To work at a wide range of absorbed dose rates by adjusting the effective volume of the detector.

The above capabilities will improve the quality of the data gathered by the customs officers during the routine inspections at the boarders and will assist the first responders in case of a radiological or nuclear emergency to estimate the exact situation.

Technology challenges

» The growth of high purity, detector grade Cd(Zn)Te crystals. Their performance will be optimized by material purification, selection of right dopants and post-growth processing to obtain high resistivity, high transport properties and homogeneous distribution of these material properties in the grown crystals. The growth of crystals with a diameter up to 75 mm will be performed.

» The fabrication of pixel detectors having structure of p-n and Schottky diodes. This will permit the application of bias voltage high enough to collect all the induced charge by both electrons and holes.

» The design of pixel electronics capable for simultaneous imaging and spectroscopy. The electronics will be bump bonded to the pixel detectors. This is essential for the localization and the identification of the radioactive source.

» The construction of a portable instrument having a stack of detecting elements.

This will allow to exploit the Compton Effect for the localization of the radioactive source and also to have variable detection efficiency.

Results

COCAE's works focused on two areas. The first was to develop a high-energy resolution and efficiency image device. The second applied techniques to locate and identify the types of radiation sources in cargo or during emergency situations.

The project resulted in the design – but not the complete construction – of a portable spectroscopic instrument focused on accurate identification and localization of radioactive sources. The instrument uses the Compton imaging technique, which deduces the energy of incident gamma ray photons and their origins by measuring energy depositions and the positions of Compton scattering interactions.

COCAE centered on the development of several core technologies

- the growth of high purity, detector grade Cd(Zn)Te crystals and the development of the first high quality ingots in Europe
- the creation of pixel detectors
- development of pixel electronics capable of recording the spatial coordinates, time of conversion, and energy levels of converted photons
- hybridization of the detectors, electronics, design, and construction of an instrument to explore the capabilities of the proposed method of radioactive source localization and identification

The intermediate results of COCAE were focused on several sectors

- Crystal growth of CdTe and CdZnTE crystals
- Device processing using the p-i-n diode structure
- Semiconductor technology for processing pixel detectors with 75 mm wafers
- Read-out electronics for pixel detectors
- Exploitation of the complete system

COCAE was tested via a large simulation effort and the development of algorithms. In the future, the project could potentially lead to the creation of a pan-European

PARTNERS	COUNTRY
Technological Educational Institute of Halkida (TEI)	Greece
Greek Atomic Energy Commission	Greece
Institute of Nuclear Physics, National Center for Scientific Research Demokritos	Greece
Oy Ajat Ltd	Finland
Freiburger Materialforschungszentrum, Albert Ludwigs Universität	Germany
Universidad Autonoma de Madrid, Departemento de Fisica de Materiales	Spain
Riga Technical University	Latvia
V.E. Lashkaryov Institute of Semiconductor Physics, National Academy of Sciences of Ukraine	Ukraine
Chernivtsi Yuri Fedkovych National University	Ukraine

CREATIF / CBRNE related testing and certification facilities - A networking strategy to strengthen cooperation and knowledge exchange within Europe

© CREATIF

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217922
Total Cost
€831,279.79
EU Contribution
€831,279.79
Starting Date
01/02/2009
End Date
31/07/2011

Coordinator

SEIBERSDORF LABOR GMBH
Radiation Safety and Applications
A-2444 Seibersdorf
Austria
Contact
Friederike Strebl
Tel: +43 (0) 50550 3265
Mobile:
+43 (0) 664 8251055
Fax: +43 (0) 50550 2502
E-mail: friederike.strebl@seibersdorf-laboratories.at
Website: http://www.creatif-network.eu

Project objectives

CREATIF's overall aim was to explore how to promote the harmonisation of national testing procedures and facilities across Europe for detection products and services in the CBRNE (chemical, biological, radiological, nuclear and explosive) sector. Among other tasks, this called for the creation of a communication platform to enable technology users, decision makers, technology providers and testers to discuss the future development of this sector. An advisory group of end-users and industrial experts was established to help shape the project's deliverables and workshops were held in which certification and testing issues regarding CBRNE detection equipment were discussed.

One of CREATIF's key objectives was to review existing testing protocols and standards in order to suggest ways to harmonise CBRNE testing, both on a geographic and technical level across the 27 EU nations, leading to a roadmap.

Results

The project's stakeholder groups agree that testing of detection systems and comparability of testing results are needed and should be based on EU agreed standards, with certification of products based on independent third party evaluation.

CREATIF's research demonstrated that complementary testing should focus on the use of real agents (or simulants) carried out in realistic operational scenarios. Training exercises for end-users should be organised to get hands-on realistic experience with detection systems. This would enhance security by providing feedback to industry to develop better detection systems and, ultimately, save public money by enabling public authorities to select the most suitable equipment.

The project also concluded that pan-EU certification would support the development of a European market for CBRNE detection systems and reduce the costs of testing.

CREATIF's main results include:

» a glossary of terms as the basis for a common language for CBRNE detection testing;

» a database on test facilities for CBRNE detection equipment;

» a report on available standards and protocols used for testing CBRNE detection systems;

» a road map for a European certification system for CBRNE sensor systems and devices, covering the following: stakeholder assessments, terminological and system descriptions, assessment of means and methods, and certification and accreditation.

In conclusion, CREATIF's research produced a broad stakeholder consensus that standardisation of testing methods is needed to boost the quality and comparability of testing results and instruments across Europe. This should be based on the development of EU-wide testing standards, followed by either international standardisation or full mutual recognition of the standards.

PARTNERS	**COUNTRY**
Seibersdorf Labor GmbH (SLG)	Austria
DGA Ministère de la Defense (DGA/MD)	France
Cotecna Inspection S.A. (COT)	Switzerland
Federal Institute for Materials Research and Testing (BAM)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands

DECOTESSC1 / DEmonstration of COunterTErrorism System-of-Systems against CBRNE phase 1

© Martijn Smeets - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242294
Total Cost
€1,587,642
EU Contribution
€1,001,627
Starting Date
01/04/2010
End Date
30/06/2011

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
Department of CBRN Protection
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
The Netherlands
Contact
Nicola Iarossi
Mark van den Brink
Tel: +31 8886 63898
Mobile: +31 6 3015 8707
Fax: +31 8886 66938
E-mail: mark.vandenbrink@tno.nl
Website: www.decotessc1.eu

Project objectives

DECOTESSC1 – a so-called 'phase one' project – set out to provide a research road-map for priorities and structures for a subsequent 'phase two' large scale Demonstration Project project, which will test effective methods for countering chemical, biological, radiological, nuclear and explosive (CBRNE) terrorist threats.

The basic idea behind DECOTESSC1 was analysis and subsequent prioritization of CBRNE counter-measure security gaps, taken as a comparison between the current situation and a theoretical ideal situation.

An in-depth background study supported this analysis, including interviews and workshops to ascertain the current threat environment and technical state-of-the-art.

Results

As well as identifying relevant research actors, technology providers, end users and other stakeholders for consultation, the project created a comprehensive Multidimensional Taxonomy System (MTS) in order to aggregate common technical terminology for this study.

This fed into a gap analysis, which eventually produced a list of 150 potential gaps in current CBRNE counter-measures. Using a ranking system, these were narrowed down to just 25 "serious" gaps in European CBRNE counter-measures.

These gaps are subdivided into five categories to be prioritized in the 'phase two' Demonstration project:

» Fusion of information and situational picture. This includes detection, identification and monitoring of actors, agents, means of delivery, targets and effects in the CBRNE field. The validity of the perceived threat and its consequences needs to be measured and verified;

» Communication. In addition to general disaster management strategies, CBRNE awareness and resilience should be increased. Aspects such as education, the role of local, regional, national and European authorities and the passive and active use of (social) media should be covered by a dedicated communication strategy;

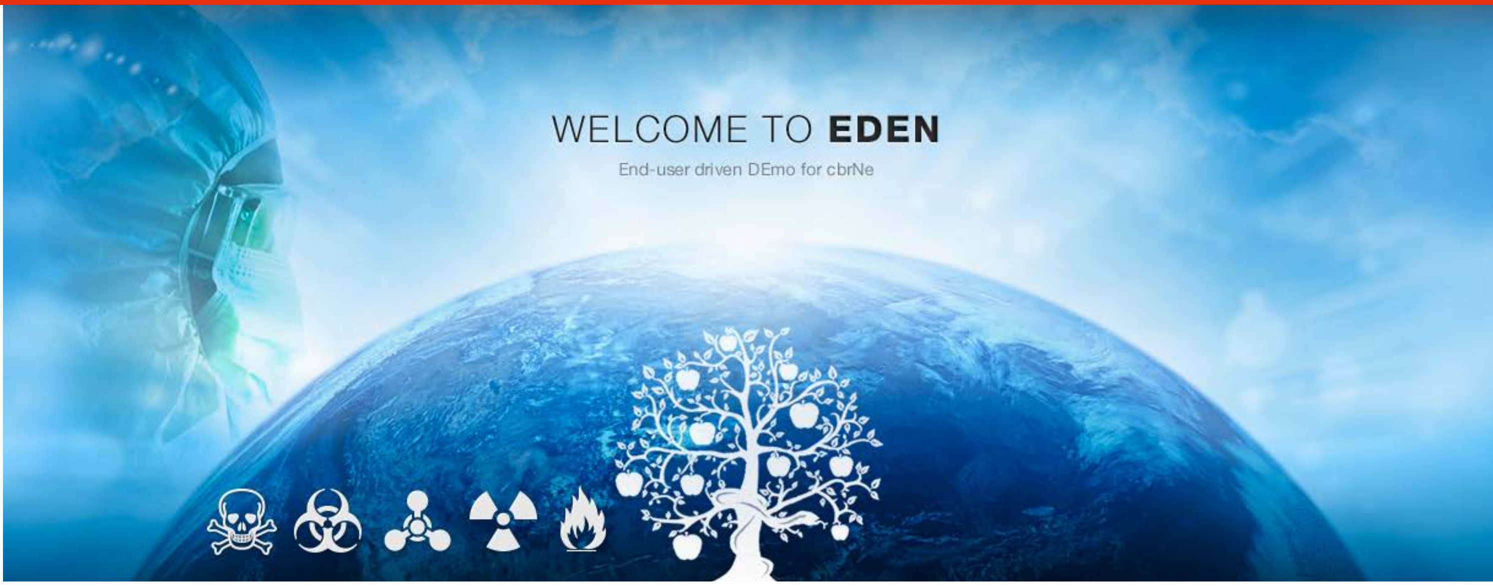
» Cooperation. This requirement includes priorities to pool resources, share (classified) information and use best practices among separate C, B, RN and E actors;

» Consequence management. Mostly post-incident activities (the response and recovery phases), but also the relationship between pre-incident activities and preparedness;

» Realistic training and exercise. In particular, new techniques (such as the use of virtual reality and serious gaming) need to be further explored, developed and demonstrated to meet both needs and restrictions.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
European Commission - Joint Research Centre (JRC)	Europe
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Fundación Tecnalia Research & Innovation (TEC)	Spain
Seibersdorf Labor GmbH (SLG)	Austria

EDEN / End-user driven DEmofor cbrNe



Information

Grant Agreement N°
313077
Total Cost
€36,075,401.17
EU Contribution
€24,826,823.91
Starting Date
01/09/2013
Duration
36 months

Coordinator

BAE SYSTEMS (OPERATIONS) LTD (BAES)
Electronic Systems
Airport works
T1F3
Rochester, ME1 2XX,
United Kingdom
Contact
Clive Goodchild
Tel: +44 (0)1634 204727
Mobile:
+44 (0)773 681 0656
Fax: +44 (0)1634 204715
E-mail: clive.goodchild@baesystems.com

Project objectives

This project intends to raise the level of maturity of the resilience capacity of EU society when it comes to CBRNe events. The project will build on the results and successful completion of previous projects and will test in the field, through key demonstrations, the validity of the solutions sought. The 36 partners of the EDEN consortium will cooperate to achieve the development of a “multi-facetted system of systems approach” that will provide an EU-tailored solution able to enhance interoperability between CBRNe operators.

A distinctive feature of the EDEN project is the activation of its end-user, SME and suppliers’ platforms. These are open bodies where end-users, SMEs or industry external to the EDEN consortium can actively take part in the project with advice and feedback. Suppliers and SMEs can offer their equipment, technologies and services relevant for CBRNe contingency plans to the EDEN project for inclusion in the “EDEN Store” and for potential demonstration during the project.

Currently, the end user platform includes 60 end users from 20 countries, while the SME platform has 34 participants and the supplier platform has 19. All platforms are expanding their capabilities by recruiting new organisations via their contact points.

Description of the work

The strategy of the work plan has been conceived along three lines, namely to:

» Allow end-users to pilot and control the whole process

» Avoid replicating topics already covered in previous projects dealing with CBRNe and thus make best use of existing projects

» Evaluate the achievements (services and performances) with concrete tests and trials essentially based on real environments and data to demonstrate affordable improvements in resilience.

The project has 4 major phases:

In the first phase end-users will define and specify the performances they need and baseline the current resilience of legacy systems. The initial societal, ethical and legal aspects will be considered.

In the second – main – phase the RTD partners will expand the PRACTICE system into the EDEN Store. Elements from other projects and new tools will be developed/matured for the EDEN demonstrations.

The third phase will entail the preparation, system integration and execution of demonstrations. There will be a combination of small, medium and large scale demonstrations based on detailed scenarios.

The fourth phase is evaluation of the demonstrations, and the societal and exploitation activities.

To exploit feedback, these 4 phases will overlap to some extent.

Expected results

The EDEN project will provide solutions to improve CBRNe resilience and allow for enhanced interoperability and effectiveness between CBRNe operators to boost the resilience of EU society.

The EDEN solutions will demonstrate the added value of large scale integration of CBRNe counter-terrorism and security solutions by improving effectiveness, efficiency, coherence, and cooperation/coordination at the national, European and international levels.

As a result, Member States and their preparedness and response organizations, large operators and local populations and media will benefit from improved integration and information sharing in countering CBRNe threats. The project will develop a "Toolbox of Toolboxes" (ToT), accessible by an exchange platform: the EDEN Store. The ToT will leverage other EU-funded CBRNe projects as well as projects funded by national research programmes and the European Defence Agency while also including new tools when needed.

PARTNERS	COUNTRY
European Commission (EC)	Belgium
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Astrium SAS (AST)	France
Forsvarets Forskninginstitutt (FFI)	Norway
Tecnoalimenti S.C.P.A (TCA)	Italy
Selex ES SPA (SES)	Italy
Université Paris XII Val de Marne (SAMU)	France
Szkoła Główna Służby Pożarniczej (SGSP)	Poland
Centre for Science, Society and Citizenship (CSSC)	Italy
Astri Polska Sp. z o.o. (APL)	Poland
Instituto Affari Internazionali	Italy
CBRNE Ltd (CBRNELTD)	United Kingdom
Universite Catholique de Louvain (UCL)	Belgium
LDI Innovation OU (LDI)	Estonia
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Teknologian Tutkimuskeskus VTT (VTT)	Finland
Fondation pour la Recherche Stratégique (FRS)	France
Indra Sistemas S.A.	Spain
L'Institut National de l'Environnement Industriel et des Risques INERIS (INR)	France
SICPA SA (SICPA)	Switzerland
Magen Davis Adom in Israel (MDA)	Israel
Przemyslowy Insytut Automatyki i Pomiarów PIAP (PIAP)	Poland
HotZone Solutions Benelux BV (HZS)	The Netherlands
Ageniza Nazionale per le nuove tecnologie, l'energia e lo sviluppo económico sostenibile (ENEA)	Italy
Societe NUCLETUDES SA (NUC)	France
OMNIDATA S.A. (OMNI)	Romania
Universidad del Pais Vasco EHU UPV (UPV/EHU)	Spain
The Univeristy of Reading (UREAD)	United Kingdom
Bruker Daltonics Limited (BRU)	United Kingdom
Ldiamon AS (LDIAMON)	Estonia
Microfuildic Chipshop GMBH (MCG)	Germany
Robert Koch - Institut (RKI)	Germany
European virtual institute for integrated risk management (EU-VRi)	Germany
Centrum Badan Kosmicznych Polskiej Akademii Nauk (SRC)	Poland
Asociacion se investigación de la industria agrolimentaria (AINIA)	Spain
Universita Cattolica Del Sacro Cuore (UCSC)	Italy
UMEA Univeritat (UMU)	Sweden
Department of Health (PHE)	United Kingdom

GIFT CBRN / Generic Integrated Forensic Toolbox for CBRN incidents

Information

Grant Agreement N°
608100
Total Cost
€7,125,972.12
EU Contribution
€5,463,924.8
Starting Date
01/09/2014
Duration
36 months

Coordinator

NETHERLANDS FORENSIC INSTITUTE
Laan van Ypenburg 6
2490 AA The Hague
The Netherlands
Contact
Daan Maas Geesteranus
Tel: +31 70 888 6128
Website:
www.giftforensics.eu

Project objectives

Forensic investigation is a key component in the fight against crime and the protection of EU societies. At present it is hampered by a lack of protocols and training in carrying out forensic analysis on CBRN-contaminated materials. The aim of GIFT-CBRN is to develop a forensic toolbox for investigating CBRN incidents. This toolbox would provide (1) procedures, sampling methods and detection of CBRN agents at the crime scene, (2) traditional forensic laboratory methods for contaminated evidence and (3) laboratory methods for profiling the CBRN agents released at the incident. The procedures and methods are will be set up and validated according to ISO17025 and the system validation will be performed by a final exercise. Procedures for chain of custody, QC to ensure the integrity of the evidence and investigations done on the evidence from crime scene to court will be developed. An education and training curriculum related to the developed procedures, best practices and methods will be designed and progressed to implementation.

Underpinning the above aims, research will be carried out to develop novel methodologies to enable traditional forensic science (DNA, fingerprint and electronic devices) to be carried out on CBRN contaminated exhibits and analytical procedures to be carried out that not only provide information about the CBRN agent itself but also through CBRN profiling provide in-depth information which can give valuable forensic information, for example points of origin.

The project team includes forensic research laboratories, potential users of the expected developments, including public and private users, and SMEs who will be able to bring the new technologies developed within the project to market

Description of the work

TGIFT will develop the most advanced forensic toolbox for CBRN incidents in the world.

The GIFT consortium intends to further develop the investigative and analytical methods that are currently only used in a secure laboratory environment and instead allow them to be used at the scene of the crime. This means ensuring not only that delicate equipment can be transported to a remote location, but that it is also able to withstand the problems of a CBRN environment such as decontamination.

Through the cooperation of Europe-wide CBRN research agencies, first responders, industrialists and subject matter experts the toolbox will provide enhanced capability in three areas of CBRN forensics;

1. Procedures, sampling methods and detection of CBRN agents at the crime scene,
2. Traditional forensic laboratory methods for dealing with contaminated evidence,
3. Laboratory methods for profiling CBRN agents released at an incident.

Expected results

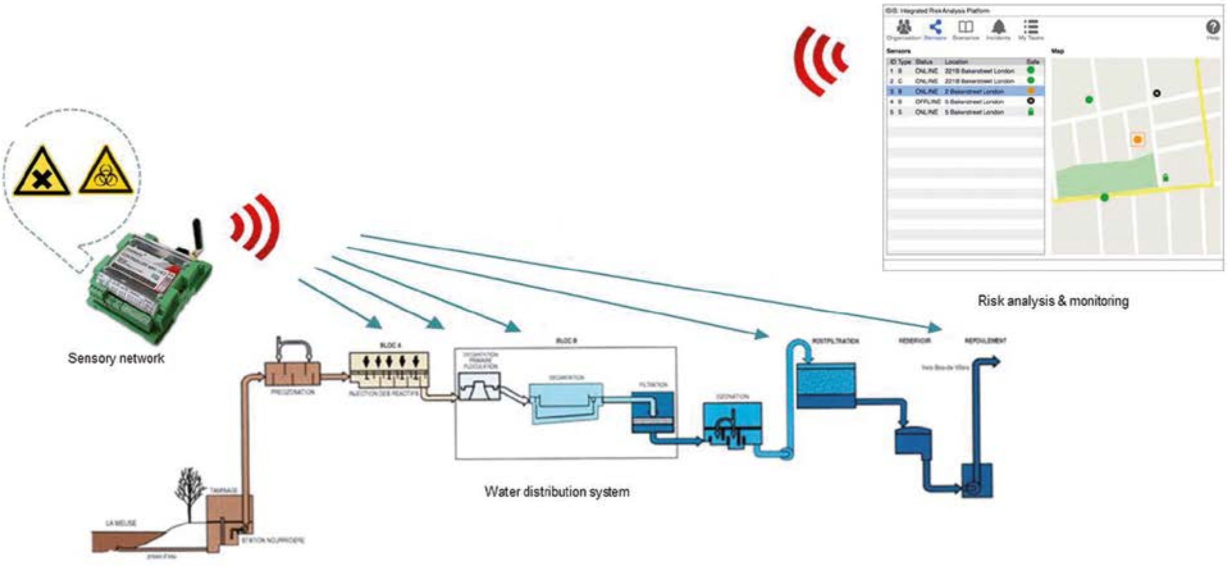
TThe GIFT consortium aims to address the issues of conducting forensic analyses in a contaminated environment by developing novel methodologies and technologies which will enable forensic investigators to perform enhanced analysis at the crime scene. Some

key innovations will be:

1. Novel sensors for chemical and biological agents
2. Detection of alpha-emitting particles using UV
3. Development of decontamination methods that won't impact on forensic traces
4. Micro-analytics on-chip to detect agents of interest
5. Attribution signatures for C, B &R agents
6. Education and training curriculum

PARTNERS	COUNTRY
FALCON COMMUNICATIONS LIMITED	United Kingdom
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK - TNO	The Netherlands
M-SQUARED LASERS LIMITED	United Kingdom
SATEILYTURVAKESKUS	Finland
DE FEDERALE OVERHEIDSDIENST JUSTITIE - LE SERVICE PUBLIC FEDERAL JUSTICE	Belgium
TOTALFORSVARETS FORSKNINGSINSTITUT	Sweden
ANALYZE IQ LIMITED	Ireland
NANOBIZ NANOBIYOTEKNOLOJIK SISTEMLER EGITIM BILISIM DANISMANLIK AR-GE LTD STI	Turkey
L.Q.C SL	Spain
JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION	Belgium
RAMEM SA	Spain
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL	Belgium
UNIVERSITY COLLEGE CORK	Ireland
ETICAS RESEARCH AND CONSULTING SL	Spain
AWE PLC	United Kingdom
SPACE APPLICATIONS SERVICES NV	Belgium
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	France
THE SECRETARY OF STATE FOR ENVIRONMENT, FOOD AND RURAL AFFAIRS	United Kingdom
RIKSKRIMINALPOLISEN NATIONAL	Sweden

ISIS / Integrated intelligent sensor system for improved security of water supplies



Information

Grant Agreement N°
312330
Total Cost
€4,790,621.90
EU Contribution
€3,484,929.00
Starting Date
01/01/14
Duration
36 months

Coordinator

C-TECH INNOVATION LTD + (CTECH)
Strategic Research
Unit 2 Capenhurst
Technology Park
CH1 6EH – Capenhurst –
United Kingdom
Contact
Domenico Cupertino
Tel: +44 151 347 2965
Fax: +44 151 347 2901
E-mail: dom.cupertino@ctechinnovation.com
Website:
www.ctechinnovation.com

Project objectives

ISIS will provide public security by developing an advanced monitoring system for drinking water networks that instantly detects chemical or biological contamination and gives clear indication of the risk level.

Description of the work

The ISIS project will combine state of the art advances in four main areas: sensors, wireless networks, intelligent surveillance strategies and integrated risk analysis software.

Expected results

» Sensors: develop four complementary innovative sensor methods. Each will have adaptable selectivity, through tailored sensing surfaces, so that collectively they can cover major potential contaminants, both chemical and biological

» Wireless network: apply new methods to achieve effective sensor distributions within the constraint of existing water system architectures

» Intelligent monitoring strategies: develop novel decision software to ensure the integrity of the monitoring system

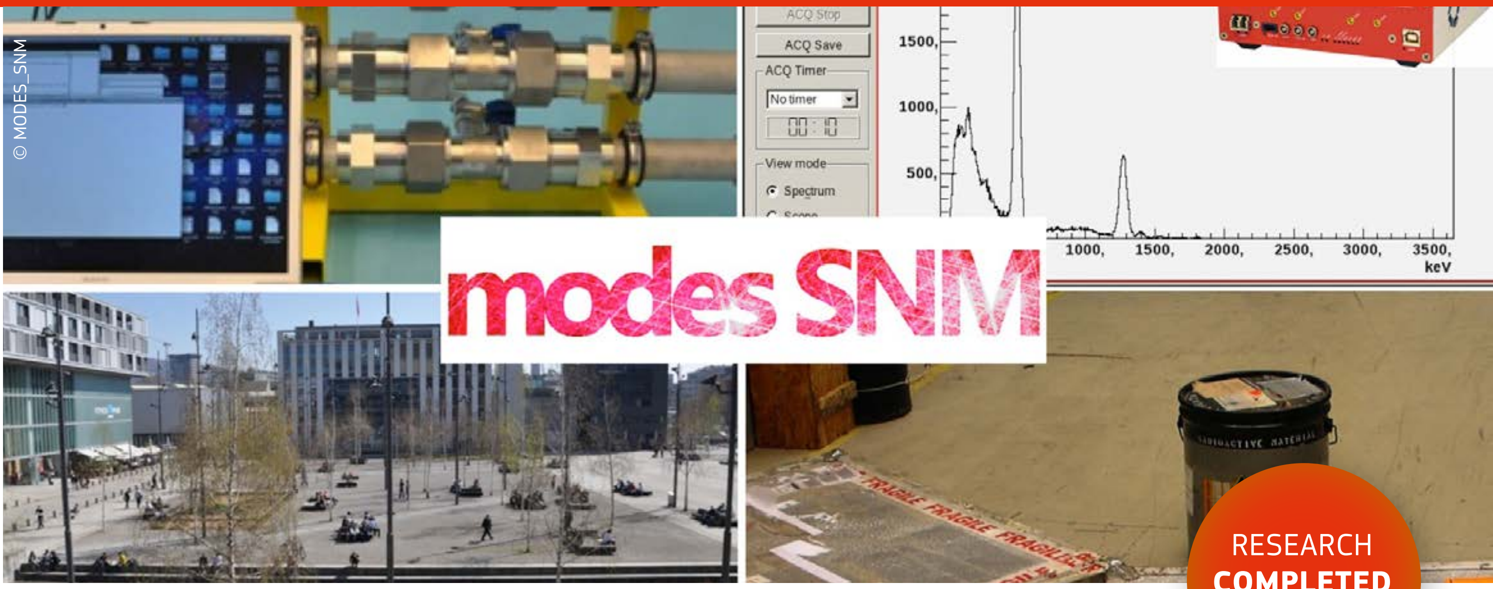
» Integrated risk analysis software: develop risk analysis software, which will be implemented in two ways.

(1) integrated into the monitoring strategy to provide a reliable model-based architecture;

(2) modelled on the existing architecture of water treatment and distribution systems in order to optimise the positioning and implementation of the sensor network.

PARTNERS	COUNTRY
European Commission (EC)	Belgium
C-Tech Innovation Ltd. (CTECH)	United Kingdom
Kauno Vandenys Uab (KV)	Lithiuania
Vivaqua Scrl (VVQ)	Belgium
Cniguard Ltd (CNIG)	United Kingdom
Advantic Sistemas Y Servicios (ADVAN)	Spain
Aleksandro Stulginskio Universitetas (ASU)	Lithuania
Commissariat à L' Energie Atomique et Aux Energies Alternatives (CEA)	France
Universitaet Wien (UNIVIE)	Austria
Universita Degli Studi Di Roma Tor Vergata (UTOV)	Italy
IOS International NV (IOS)	Belgium

MODES_SNM / Modular detection system for special nuclear material



RESEARCH **COMPLETED**

Information

Grant Agreement N°
284842
Total Cost
€3,282,051.20
EU Contribution
€2,411,633
Starting Date
01/01/2012
End Date
30/06/2014

Coordinator

UNIVERSITA' DEGLI STUDI DI PADOVA
Department of Physics and Astronomy
Via Marzolo 8
35131 Padova, Italy
Contact
Giuseppe Viesti
Tel: +39 0498275933
Mobile: +39 3484115826
Fax: +39 0498275961
E-mail:
giuseppe.viesti@unipd.it
Website:
http://www.fisica.unipd.it/

Project objectives

Special Nuclear Materials (Highly Enriched Uranium and Plutonium) are difficult to detect, especially when masked or shielded: gamma rays and neutrons emitted by SNM have to be detected in order to increase the sensitivity against natural backgrounds. These objectives were pursued by optimizing a novel technology recently developed allowing the detection of all relevant radiation types and the engineering of a prototype of a modular, compact, mobile detection system that was qualified under laboratory conditions. Moreover, it was commissioned in an on-field campaign driven by the end-user group established in the project. The campaign focused on both performance and usability aspects including the verification of the man-machine interface. The MODES_SNM system satisfied two major requirements:

- improving the state-of-the-art in detection of radioactive and Special Nuclear Material in terms of sensitivity for shielded SNM;
- being usable by emergency responders in the field filling the gap between Radiation Portal Monitors and hand-held devices.

Description of the work

Starting from the pre-existing know-how of ARKTIS in the field of high pressure noble gas scintillation detectors, the MODES_SNM project aimed first at a general optimization of the detector with the goal of designing and realizing the modular mobile system described below. The relevant tasks were:

- Optimization of the mechanical design of the high-pressure gas cells to minimize weight;
- Studies and development geared towards the replacement of the photomultipliers in the current system with solid state devices to reduce the size and increase robustness;
- Design of compact front-end electronics based on CAEN know-how on Digital Pulse Processing.

In parallel with the optimization task, two other tasks were performed:

- Using ARKTIS technology, new types of detectors were developed using noble gas cells: a gamma ray sensor and a thermal neutron sensor. The ambitious goal of this task was to develop a suite of detectors capable of gamma, fast and thermal neutron detection, and spectroscopy, all based on the same technology and using the same electronics front-end and DAQ;
- A suitable INFORMATION SYSTEM (IS) was prepared. The IS managed and controled the detectors, including start-up operations and calibrations. It managed and analyzed the data flow from the detectors to achieve on line: 1) the irate of all radiation species compared with the background level; 2) the application of energy windowing on the fast-neutron and gamma-ray spectra to validate the alarms for weak sources; 3) the analysis of gamma ray spectra for isotope identification; 4) data fusion of all detectors and presentation of the data to the operator through a simple man-machine interface.

This MODES_SNM prototype represented the final deliverable of the project. It was modular and scalable, divided into so-called system blocks easily mounted and removed into/onto vehicles:

- *Block A* consisted of all system electronics including power supply and battery, signal processing electronics and computing;

» *Blocks B* consisted of arrays of four detectors per block, selected from the suite of gamma, fast and thermal neutron. The prototype consisted of one *Block A* and several *Block Bs,* depending on the specific deployment.

Results

The MODES SNM prototype was qualified during 2014 for the detection of moving gamma-ray and neutron sources as well as for the detection and identification of 252Cf, (alpha,n) neutron sources, Pu and U samples at the PERLA Laboratory at JRCIspra. It was then tested on the field at the Rotterdam and Dublin seaports, at the Heathrow Airport, and in Basel and Uri (Switzerland).

Results from the field tests demonstrated that the MODES SNM prototype was shown to be very robust, surviving all transportations over more than 6000 km and end-user operations under different conditions. The end-users were able to run the system without problems and without the supervision of technical experts. The prototype showed great potential since the beginning; its detection performances proved to be comparable and in some cases even surpassing those of commercial systems, while providing additional features which are of high importance to customers. The demonstration campaign showed only one relevant issue concerning the occasional triggering of false alarms, a problem identified and solved at the end of the field tests. At this time the prototype is capable of detection and identification of gamma-ray sources and NORMs, neutron sources as 252Cf, Am/Be, Pu/Be and SNM as Pu and U samples. The system also detects the presence of hydrogenated or lead shielding enclosing neutron sources.

PARTNERS	COUNTRY
UNIVERSITA DEGLI STUDI DI PADOVA (UNIPD)	Italy
ARKTIS RADIATION DETECTORS LTD (ARKTIS)	Switzerland
Narodowe Centrum Badań Jądrowych - National Centre for Nuclear Research (NCBJ)	Poland
Eidgenössische Technische Hochschule Zürich (ETH)	Switzerland
COSTRUZIONI APPARECCHIATURE ELETTRONICHE NUCLEARI C.A.E.N. SPA (CAEN)	Italy
UNIVERSITA DEGLI STUDI DELL'INSUBRIA (UINS)	Italy
THE REVENUE COMMISSIONERS (RC)	Ireland
THE UNIVERSITY OF LIVERPOOL (UNILIV)	United Kingdom

REWARD / REal-time Wide-Area RaDiation Surveillance System

© Andrea Danti, Benjamin Haas û fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284845
Total Cost
€4,270,883
EU Contribution
€3,020,795
Starting Date
01/12/2011
End Date
30/11/2014

Coordinator

CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS
Instituto de Microelectrónica de Barcelona, IMB-CNM (CSIC)
Campus Universidad Autónoma de Barcelona
08193 Bellaterra
(Barcelona), Spain
Contact
Prof. Manuel Lozano
Tel: +34 93 594 77 00
Fax: +34 93 580 14 96
E-mail:
Manuel.Lozano@csic.es
Website:
http://www.reward-project.eu/

Project objectives

The REWARD project developed portable, intelligent radiation detectors that can determine the flux and energy of the incoming radiation, as well as their own location. Multiple individual detectors were integrated in a ubiquitous radiation sensing system in order to continuously monitor an area, generate an alarm if an anomalous situation is encountered and locate and identify the radiation sources. The main features of the REWARD system:

» Real-time system with wide area coverage;

» Novel solid-state detector technologies;

» Gamma and neutron detection;

» Scalable in terms of complexity and costs;

» Portable and adaptable to any type of environment.

New methods and tools were developed for fusion, real-time and offline data mining of the radiation sensor information to discover patterns and associations of background radiation.

Description of the work

REWARD is a novel mobile system for real-time, wide-area radiation surveillance. It is based on the integration of new miniaturized solid-state radiation sensors: a CdZnTe detector for gamma radiation and a high-efficiency neutron detector based on novel silicon technologies. The sensing unit has included a wireless communication interface to send the data remotely to a monitoring base station as well as a GPS system to calculate the position of the tag.

The system also incorporated middleware and high-level software to provide web-service interfaces for the exchange of information and an expert system to continuously analyse the information from the radiation sensor and correlate it with historical data in order to generate an alarm when an abnormal situation is detected.

REWARD was useful for many different scenarios such as nuclear terrorism threats, lost radioactive sources, radioactive contamination or nuclear accidents. It can be deployed in emergency units and in general in any type of mobile or static equipment, but also inside public/private buildings or infrastructures. The sensing units have been highly portable thanks to their low size and low energy consumption. The complete system was scalable in terms of complexity and cost and offered very high precision in terms of both the measurement and the location of the radiation.

REWARD's goals were realized by the collaborative effort of eight highly specialized, though synergistic research organizations, wireless sensor networks providers, software developers and application users.

The modularity and flexibility of the system allowed for a realistic introduction to the market. Authorities may start with a basic, low-cost system and increase the complexity based on their evolving needs and budget constraints.

Results

REWARD delivered a system composed of the following main elements:

» High efficiency CdZnTe detector for gamma radiation and neutron detector based on novel silicon technologies integrated in the same monitoring tag to make it easier to identify both radioactive sources and nuclear materials.

- A central monitoring and decision support system developed with the ability to process data from the sensing units and to compare them with historical records.
- A cloud-based middleware for the management and communication of the wireless sensor network with the central monitoring and decision support system that is fully scalable to handle from a single tag.
- A security framework to ensure protection against unauthorised access to the network and data, ensuring the privacy of the communications and contributing to the robustness of the system.

Special emphasis was given to engage end users, stakeholders and investors coming from academia, large industries, SMEs, and security forces through different dissemination activities.

Research, demonstration, dissemination, and exploitation resulted in technological advances that are expected to have a significant impact on Europe's CBRN security. REWARD constitutes a new tool for detecting difficult to detect radioactive sources and nuclear materials, having a direct impact on the goals of the EU CBRN Action Plan.

PARTNERS	**COUNTRY**
Consejo Superior de Investigaciones Científicas (CSIC)	Spain
Sensing & Control Systems S.L. (S&C)	Spain
Vitrociset S.p.A (VCT)	Italy
Universität Freiburg (ALU-FR)	Germany
Instituto Tecnológico e Nuclear (ITN)	Portugal
XIE. X-ray Imaging Europe (XIE)	Germany
EDISOFT (EDI)	Portugal
Civil Protection Unit of Campania (DIP)	Italy

SAFEWATER / Innovative tools for the detection and mitigation of CBRN related contamination events of drinking water

Information

Grant Agreement N°
312764
Total Cost
€4,776,382.20
EU Contribution
€3,494,338.25
Starting Date
01/10/2013
Duration
39 months

Coordinator

ARTTIC (ART)
ARTTIC
58A rue du Dessous des Berges
75013 Paris, France
Contact
Anna Ellinge Madar
Tel: +97233732010
Mobile: +972526604919
Fax: +9723732009
E-mail: ellinge@arttic.eu
Website: www.arttic.eu

Project objectives

The overarching aim of the SAFEWATER project is to develop a comprehensive and pragmatic platform to manage the safety and security of drinking water, reducing the time to react and effectively respond to a crisis.SAFEWATER will thus cover the detection, response, and recovery stages of potential events.

SAFEWATER will pursue the following objectives:

» OB1: Improve preparedness through enhanced event detection capabilities, including virtual sensors machine learning algorithms and unsupervised learning capabilities to train the system;

» OB2: Strengthen current response & recovery capacities of security and safety management systems for drinking water through a new generation of real-time decision support systems;

» OB3: Develop new and improve current CBRN sensors for drinking water;

» OB4: Develop adequately focused solutions for different usage contexts;

» OB5: Optimise internal efficiency and external impact.

Description of the work

The SAFEWATER project will be driven by concrete usage cases corresponding to potential water security events. To make sure that the project is efficiently managed, the consortium will work according to common global milestones, which structure the project in a set of V1 solutions (Release 1 at midterm), including:

» the integration and development of partial capabilities (sensors, system, and Event Management System);

» Initial testing results, including a SAFEWATER user workshop

and V2 solutions (Release 2 at the end of the project), including;

» the integration and development of full capabilities (sensors, system, and Event Management System) based on the outcomes of testing and further technologicl developments;

» physical trials;

» final results culminating in a final workshop.

Expected results

The SAFEWATER solution fully covers the variety of drinking water security management situations (detection, response, and mitigation) and develops cutting-edge modelling methods, which will enable a near real-time overview of the water networks in large urban areas.

With the development of better and smarter technological solutions such as online CBRN detection, spatial modelling and look-ahead simulations, SAFEWATER will provide reliable tools for the management of drinking water crises.

During its second and final release of technology, SAFEWATER will provide adequate tools to enhance the online detection capabilities of the presence of contaminants in all water networks, and to effectively alert crisis managers, decision makers, and the general public in due time.

Additionally, it will introduce a paradigm shift in the overall management of water quality parameters by investigating the domestic sensors solution – through the testing and selection of adequate low cost, and low maintenance sensors, and by adjusting the Event Detection System capacities to handle signals from a large number of distributed domestic sensors

The expected impact of SAFEWATER will, however, go far beyond water security: its open systems approach and deployed technologies will be useful for drinking water quality management in general. Indeed, aside from CBRN attacks perpetrated by malevolent actors, whose probability is low, the contamination of drinking water by sewage or human error is more likely but no less disastrous. Thus SAFEWATER can respond to the needs of utilities to protect their networks from all kind of contaminations.

PARTNERS	**COUNTRY**
ARTTIC (ART)	France
Hagihon Company Ltd. (Hagihon)	Israel
3S Consult GMBH (3S)	Germany
Fraunhofer-Gesellschaft Zur Foerderung der Angewandten Forschung E.V (Fraunhofer IOSB)	Germany
Aguas do Algarve, SA (AdA)	Portugal
Commissariat A L Energie Atomique et aux Energies Alternatives (CEA)	France
ACREO Swedish ICT AB (ACREO)	Sweden
Decision Maker Ltd (DM)	Israel
BioMonitech Ltd (BM)	Israel

SCINTILLA / Development of detection capabilities of difficult to detect radioactive sources and nuclear materials

© CEA

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285204
Total Cost
€3,867,616.38
EU Contribution
€3,023,652.12
Starting Date
01/01/2012
End Date
31/12/2014

Coordinator

COMMISSARIAT À L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
DRT/LIST/ DCSI/ LCAE
CEA Saclay, Bât 516,
Point courier n°72
91191 - Gif sur Yvette -
France
Contact
Guillaume SANNIE
Tel: +33 1 69 08 51 88
Fax: +33 1 69 08 60 30
E-mail:
guillaume.sannie@cea.fr

Project objectives

SCINTILLA aimed at building an innovative and comprehensive toolbox of devices and best-of-breed technologies for the enhanced detection and identification of difficult to detect radioactive sources and nuclear material:

» Dealing with the challenge of masked and shielded material;

» Developing effective solutions, which are reliable, portable/mobile and cost effective;

» Finding a reliable replacement for Helium-3, which is the major consumable for today's RPM (Radiation Portal Monitors) devices for neutron detection and has become close to unavailable in the European Union.

Description of the work

SCINTILLA covered a broad range of different usage cases including automatic screening of moving targets such as people, cars and trucks, the inspection of large containers as well as the detection of radioactive sources in bombs.

The SCINTILLA Test-bed Service and annual Technology Benchmarks respectively supported and selected the technologies; they were also open to third-party developments.

In addition to more technical criteria such as sensitivity, discrimination between neutron and gamma radiation and the minimisation of false alarms, SCINTILLA assessed technologies with respect to practical criteria such as portability, mobility and cost-benefit ratios.

The resulting selection of best-of-breed technologies was then integrated into full prototype devices, which were ready for assessment in selected usage cases under (close to) real-life conditions.

To reflect the different TRL of technologies under development the project proceeded in two stages with usage assessments at midterm and project end.

The SCINTILLA Toolbox was provided with User Guidelines and a Technology Handbook for integrators.

SCINTILLA also developed and promoted communication protocols and standards.

Around the Test-bed and Benchmark services a sustainable SCINTILLA Partnership Network was built, a worldwide community of technology providers, experts and users, around the topic of detection technologies.

Results

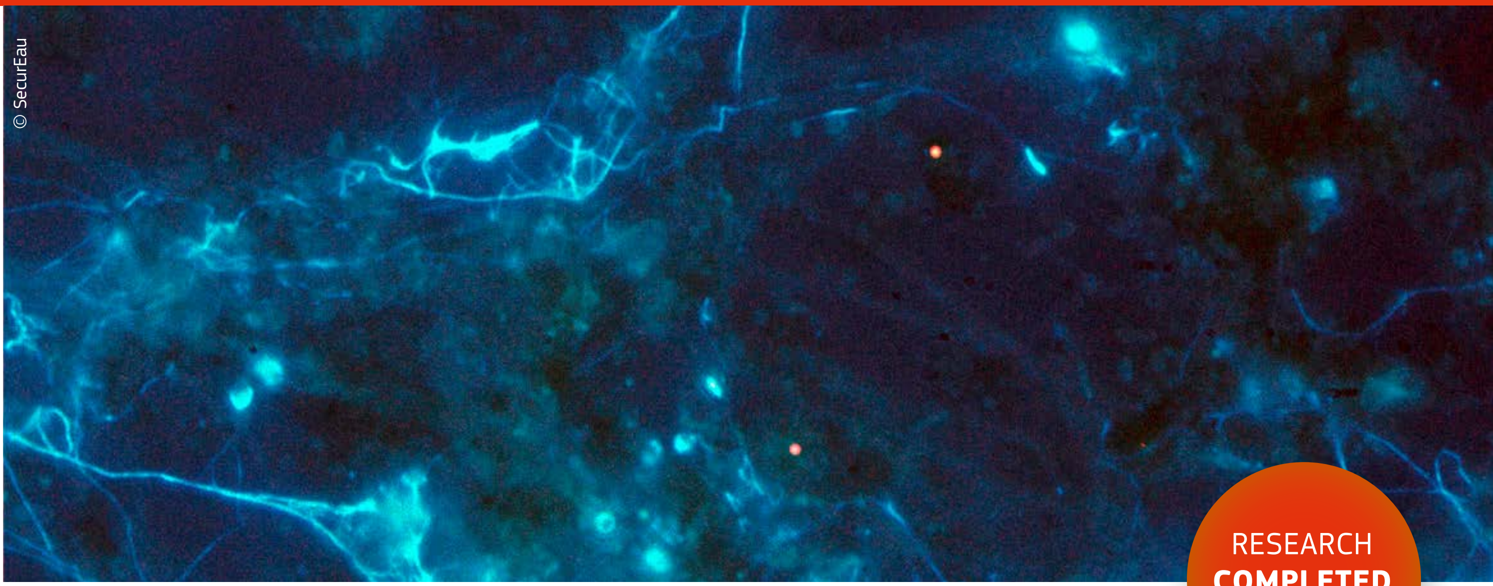
SCINTILLA developed a toolbox featuring new and improved scintillator-based technologies for the passive detection of difficult-to-detect radioactive sources and nuclear materials, which may threaten EU citizens and society. SCINTILLA helps address the strategic issue to Europe by replacing He3 for neutron detection.

The SCINTILLA Testbed services and Technology Benchmarks assured that the SCINTILLA Toolbox stayed open to best-of-breed technologies and new developments. The iterative process allowed regular improvements of developments and prototypes. Regular interaction with end-users allowed the consortium to match market constraints and demand.

3 patents were submitted by consortium partners: n°13 58552 (CEA), n° 14 60162 (CEA) and PCT/IB2014/065876 (INFN/ANSALDO). Commercial exploitation includes improved detection portals from SYMETRICA and INFN/ ANSALDO. Some of the portal detectors have already been successfully sold into major international contracts. The testing facilities at EK and JRC will continue to serve the purpose of testing and certifying detection equipment to deal with difficult-to-detect sources and nuclear materials.

PARTNERS	COUNTRY
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
ISTITUTO NAZIONALE DI FISICA NUCLEARE (INFN)	Italy
ANSALDO NUCLEARE SPA (ANSALDO)	Italy
CENTRE FOR ENERGY RESEARCH – HUNGARIAN ACADEMY OF SCIENCES (IKI)	Hungary
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V (FhG INT)	Germany
ARTTIC (ART)	France
SAPHYMO SAS (SAPHYMO)	France
SYMETRICA SECURITY LTD (SYMETRICA)	United Kingdom

SECUREAU / Security and decontamination of drinking water distribution systems following a deliberate contamination


© SecurEau

RESEARCH COMPLETED

Information

Grant Agreement N°
217976
Total Cost
€7,481,418.73
EU Contribution
€5,266,871
Starting Date
01/02/2009
End Date
31/01/2013

Coordinator

UNIVERSITE HENRI POINCARE - NANCY 1
Service des Relations Internationales, Cellule Europe
22-30 rue Lionnois
60120
54003 Nancy cedex
FRANCE
Contact
Sylvain FASS
Tel: +33 (0)3 54 50 54 37
Fax: +33 (0)3 54 50 54 01
E-mail:
sylvain.fass@uhp-nancy.fr
Website:
http://www.secureau.eu/

Project objectives

The main objective of this proposal is to launch an appropriate response for rapidly restoring the use of the drinking water network after a deliberate contamination and by way of consequence to limit the impact on the population of safe water privation because of contaminated networks. Five main topics will be addressed:

» Detection of unexpected changes in water quality;

» Adaptation of analytical methods to rapidly detect specific CBRN contaminants;

» Localization of the point source(s) of contamination;

» Decontamination procedures of the distribution system;

» Controlling the efficacy of the corrective actions.

Description of the work

SecurEau will implement an effective and timely response to a CBRN attack. Questions that will be addressed for successful coordinated response of water utilities and regulatory agencies to contamination include:

» Detection of unexpected changes in water quality which could be in relation to a deliberate contamination event, by applying commercially available or recently developed generic sensors placed throughout the distribution systems;

» Adaptation of known analytical methods to rapidly detect specific CBRN contaminants in water and especially in biofilms and on pipe walls;

» Localization of the point source(s) of contamination and subsequently the contaminated area (via modelling reactive transport) allowing delimitation of the corrective actions;

» Decontamination procedures (efficient and realistic) of the distribution system, i.e. adapted to size, age, architecture of the network, including the treatment of water extracted from the system and used for washing the pipe wall;

» Controlling the efficacy of the corrective actions by analysing the water bulk and especially the pipe walls' surface and the deposits;

» The case studies will give the chance for the practitioners to apply on site in realistic conditions the selected sensors, software and remediation technologies. It is a unique occasion to test an emergency procedure on a complicated, quasi directly inaccessible, and relatively fragile system, to evaluate its feasibility at field scale, and to evaluate the difficulty in applying corrective treatments to the huge water bulk generated by the neutralisation/extraction of contaminants.

Results

The project developed sensors and specific contingency plans to identify and address the contamination of water in urban and rural water distribution networks.

SECUREAU achieved 10 important technological advancements:

1. sensors that detect any abnormal changes in water quality and provide assistance to the operator to manage the drinking water network
2. software that identifies the optimal location of water quality sensors and data treatment
3. mathematical models to find the optimal distribution of sentinel coupons
4. mathematical approaches to identify sources of contamination and the contaminated areas

5. CBRN pollutant analytical methods
6. modeling sorption and desorption to predict the spread of contamination
7. pipe wall cleaning and decontamination
8. methods of handling of decontamination sludge and water
9. verification of decontamination by deposits, biofilms or scale analysis, or by using sensor signals
10. decision tools within organizational frameworks and methodologies to follow in specific crisis situations.

Building on the above tasks during its fourth and final year, SECUREAU carried out experiments on wall deposits and biofilms to determine the kinetic parameters for absorption and desorption of contaminants, and methods for decontaminating water and cleaning pipes. It also used software to model the contamination of drinking water networks and identify contamination sources.

Finally, the research team installed two networks – one rural, one urban – comprised of 40 sensors to collect field information and to create an early warning system of contamination.

PARTNERS	COUNTRY
Université Henri Poincaré – Nancy 1 (UHP)	France
Centre National de la Recherche Scientifique (CNRS)	France
Veolia Environnement Recherche et Innovation (VERI)	France
Rheinisch-Westfälisches Institut für Wasserforschung gemeinnützige GmbH (IWW)	Germany
University of Southampton (SOTON)	United Kingdom
Faculdade de Engenharia da Universidade do Porto (FEUP)	Portugal
Riga Technical University (RTU)	Latvia
Centre national du Machinisme Agricole, du Génie Rural, des Eaux et des Forêts (CEMAGREF)	France
Commissariat à l’énergie atomique et aux énergies alternatives (CEA)	France
Monitoring Systems Ltd. (MSystems)	United Kingdom
Veolia Water Central (VWC)	United Kingdom
Radiation and Nuclear Safety Authority (STUK)	Finland
Kelda Group PLC (YWS)	United Kingdom
National Institute for Health and Welfare (THL)	Finland

SNIFFER / Securing the food chains from primary production and animal feeds to consumer-ready food against major deliberate, accidental or natural CBRN contamination.

© Thinkstock

Information

Grant Agreement N°
312411
Total Cost
€3,632,513
EU Contribution
€2,720,029
Starting Date
01/05/2013
Duration
36 months

Coordinator

TEKEVER ASDS (TEK)
TEKEVER ASDS
Rua das Musas 3.30
1990-113, Lisboa
Portugal
Contact
André Oliveira
Tel: +351 213 304 300
Fax: +351 213 304 301
E-mail:
andre.oliveira@tekever.com

Project objectives

Project SNIFFER envisions the design and development of a network of distributed detection devices, capable of rapid, on-site detection of multiple kinds of agents and CBR agents with high sensitivity and specificity throughout the most vulnerable stages of the food supply chain (such as farms, large collection centers, wholesalers, etc...).

The project will address both available sensor technology and new, complementary sensor devices that shall be used for the detection of hazardous CBR agents within the food supply chain. The sensor devices to be developed are characterised by their portability, ease of use and reusability. Another important feature of the new device will be its modular design, i.e. the device is formed by several independent modules (sensors, communication device, on-board computing, etc), combined through generalized and standardized connections.

The network of sensor devices will be designed as a centralised architecture, in which all the data from the devices will be sent to a command center. An operator of the SNIFFER system will also have the ability to remotely control and command the sensor devices using a specific interface from the command center.

Project SNIFFER also envisions the creation of a set of guidelines, which presents the countermeasures and procedures that shall be used within the European Union whenever a food or feed borne incident is detected within the food supply chain. The guidebook will provide help to the appropriate entities in employing the corrective counter-measures in order to mitigate, restrain or ultimately eradicate the hazardous agent.

The aforementioned objectives of the project will be directed to achieve the final goal of providing means of countermeasure to mitigate a possible incident of CBR health hazardous agents in the food supply chain and to increase the security within all the steps that constitute the food supply chain.

Description of the work

The SNIFFER consortium has established a precise and main objective for this project which is to:

» Increase the security of the food supply chain by developing a network of detection devices to detect CBR agents introduced in food either by accidental, natural or intentional means.

This achievement will be pursued by providing specific outcomes from the activities identified below:

» Development of a new sensor (MIPs technology) with a faster detection time, and improved re-usability

» Combination of MIPs with fluorogenic probes to reduce false positive rates and improve sensor robustness

» Provide the capability to network different sensors at different stages/locations of the food supply chain (vertical and horizontal dimensions)

» Development of the capability to improve the quality of detection through data fusion

» Definition of a set of sample preparation procedures

» Definition of a set of recommendations to policy makers (specific recommendations to food security agencies and European authorities)

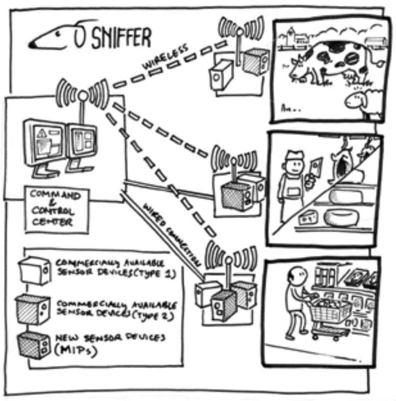
» Definition of a set of scenarios specifically adapted to food supply chain and the SNIFFER validation methodology

Expected results

The capability to network different devices with different functionalities (i.e. capable of detecting different agents) throughout the entire food supply chain will undoubtedly reduce the detection time (the time between contaminating a specific food and detecting this contaminated food somewhere along the chain) of contaminant agents, introduced either deliberately, accidentally or through natural sources.

By providing users with the ability to perform tests at any stage across the entire food chain (which is basically already possible but not with the technology proposed in SNIFFER), the probability of detecting contamination earlier will increase.

Additionally, the faster detection time and higher rate of re-usability introduced by the MIPs technology will enable users to perform more tests/hour and wait less time for the results which again results directly in lower detection times.


SNIFFER
WIRELESS
COMMAND & CONTROL CENTER
WIRED CONNECTION
COMMERCIALLY AVAILABLE SENSOR DEVICES (TYPE 1)
COMMERCIALLY AVAILABLE SENSOR DEVICES (TYPE 2)
NEW SENSOR DEVICES (MIPs)

PARTNERS	COUNTRY
Tekever ASDS (TEK)	Portugal
Ministério da Defesa Nacional (LBDB)	Portugal
Umea Universitet (UMU)	Sweden
INESC Porto – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC)	Portugal
Universidad de Burgos (UBU)	Spain
Osterreichische Agentur für Gesundheit und Ernahrungssicherheit (AGES)	Austria
Centre Suisse d'electronique et de microtechnique SA – Recherche et developpement (CSEM)	Switzerland
Forvarets Forskninginstitutt (FFI)	Norway

SPICED / Securing the spices and herbs commodity chains in Europe against deliberate, accidental or natural biological and chemical contamination

© BfR

Information

Grant Agreement N°
312631
Total Cost
€4,586,455.60
EU Contribution
€3,499,942.35
Starting Date
01/07/2013
Duration
36 months

Coordinator

FEDERAL INSTITUTE FOR RISK ASSESSMENT (BFR)
Department Biological Safety
Max-Dohrn-Straße 8-10
Postfach 126942, 10609 Berlin
10589 Berlin
Germany
Contact
Prof. Dr. Bernd Appel
Tel: +49 30 18412 2151
Fax: +49 30 18412 2951
E-mail: spiced@bfr.bund.de
Website: www.spiced.eu

Project objectives

Securing food chains against deliberate, accidental or natural contaminations is directly related to the safety of food products.

Many alerts from European countries via the Rapid Alert System of Food and Feed (RASFF) over the past years have included spices and herbs. Additionally, these components are contained in almost every processed food, including ready-to-eat products. Thus consumers can be directly exposed to contaminated spices and herbs. There is a need to monitor these commodities. SPICED's objectives are to:

» characterize the heterogeneous matrices of spices and herbs and their respective production and supply chains regarding relevant biological and chemical hazards that can lead to major deliberate, accidental or natural contaminations in the food supply chain;

» improve the knowledge of biological hazard properties as well as on-site and high throughput diagnostic methods for appropriate detection;

» reduce (industrial) chemical adulterations and ensure authenticity of spices and herbs by evaluating and improving non-targeted fingerprinting methods;

» improve alerting, reporting and decontamination systems as well as techniques to ensure prevention and response on high quality level.

The consortium will evaluate the most important spices and herbs that could be the source for natural, accidental or deliberate contaminations.

Description of the work

WP1, "Management and Coordination", includes scientific management and assessment of progress and results, financial and administrative management, intra-consortium communication and management of gender issues.

WP2, "Matrix Chains and Modelling", will systematically collect and evaluate information about spices and herbs production steps and the potential hazard of contamination. Vulnerable points along the spices and herbs production chain will be identified. An evaluation of various parameters will determine the risks and the potential of possible interventions.

WP3, "Biological Hazards", will improve the knowledge about microorganism properties (e.g. tenacity) and their detection. Current microbiological and molecular techniques, including existing sample preparation, purification and detection methods will be investigated for the development of reliable and standardized cultural, on-site screening as well as high throughput approaches. A database will be created to include data on biological hazard properties and diagnostic methods.

The aim of WP4, "Chemical Hazards", is to develop a rapid and cost-efficient set of methodologies for the detection of spices and herbs contamination with (unexpected) chemical agents. Fingerprinting data will be used to develop and evaluate various chemometric (one-class) classification techniques that allow distinguishing authentic (non-adulterated) samples from adulterated/contaminated samples.

In WP5, "Prevention and Response", alerting and reporting systems and decontamination techniques will be investigated, with recommendations to be published. Moreover, a guideline for differentiation between natural and intentional incidents will be developed.

WP6, "Sustainability and Dissemination", deals with the dissemination of knowledge to the public, governmental institutions and scientific and industrial communities.

Expected results

The SPICED project will lead to a better and more comprehensive view of the heterogeneous matrix of spices and herbs. Its approach should lead to improved food safety and food security aspects in the spices and herbs food chain, and to reduce human casualties and the economic impact. The EU level of expertise in this field will be significantly increased.

PARTNERS	COUNTRY
Federal Institute for Risk Assessment (BfR)	Germany
Austrian Agency for Food and Health (AGES)	Austria
Institute of Food Safety, Animal Health and Environment (BIOR)	Latvia
DLO foundation - RIKILT (DLO)	The Netherlands
Fuchs Gewürze GmbH (FUCHS)	Germany
National Agricultural Research and Innovation Center (KEKI)	Hungary
RTD Services (RTDS)	Austria
University of Limerick (UL)	Ireland
National Agricultural and Food Center (VÚP)	Slovakia
Bundeswehr Research Institute for Protective Technologies & NBC-Protection (WIS)	Germany
Wageningen University (WU)	The Netherlands

TAWARA_RTM / TAp WAter RAdioactivity Real Time Monitor

Information

Grant Agreement N°
312713
Total Cost
€3,414,864.80
EU Contribution
€2,564,554.00
Starting Date
01/12/2013
Duration
30 months

Coordinator

UNIVERSITA' DEGLI STUDI DI PADOVA (UNIPD)
Department of Physics and Astronomy
via Marzolo, 8
I-35131 – Padova - Italy
Contact
Marcello Lunardon
Tel: +39 049 827 5643
Fax: +39 049 827 7102
E-mail:
marcello.lunardon@unipd.it
Website: www.tawara-rtm.eu

Project objectives

The main purpose of the TAWARA_RTM project is to create a platform for drinking water security against deliberate or accidental radiological or nuclear threats.

This goal will be pursued by targeting the needs of the Warsaw Waterwork Company MPWIK, but it will be easily adapted to other large municipalities in Europe and abroad.

The proposed prototype will be composed of two main radioactivity detection systems: a real-time monitor system (RTM) for the measurement of the gross alpha and beta activity in the water, and a spectroscopic system (SPEC) for the identification of the radioactive contaminant by exploiting the recognition of its characteristic gamma lines. An additional gamma detection system for early alarm in case of strong radioactive contaminations of raw water will be added to the monitoring network in order to preserve as much as possible the water treatment plant by blocking the contaminated water at its intake.

As required in the call topic, the project will cover the development, assessment, demonstration, deployment and monitoring phases of the new monitoring system at the North Warsaw site where the prototype will be deployed.

TAWARA_RTM's mechanical lay-out, electronics architecture and information system will be specifically conceived for easy integration of additional specialized sensors for chemical or biological threats.

In this way TAWARA_RTM will offer a system for real time on-site monitoring of water quality that will be useful in the following tasks:

» early warning in case of changes in the radioactive content of water and time reading of the changes;

» fast alarm for crossing thresholds that require rapid actions for the tap water distribution system;

» in case of alarm, starting the spectroscopic investigation to determine the type of contamination and decide the appropriate and effective countermeasures (response and mitigation measures).

Description of the work

Starting from the project consortium's pre-existing know-how regarding the use of scintillation detectors in nuclear physics applications, TAWARA_RTM's work plan foresees first an R&D phase where available detectors and technologies will be optimized for integration into this new application.

The relevant tasks comprise:

» design and production of TAWARA_RTM's prototype RTM detector to continuously measure on site the water's gross alpha and beta activity. The detector is based on an array of commercially available plastic scintillators that distinguish between alpha and beta signals. However, these kind of detectors have never been used so far for such application. The optimal read-out scheme and a suitable water-protection and functionalization treatment of the scintillator surface will be realized during the initial R&D phase of this task. Moreover, the additional gamma detection system for early alarm in case of strong radioactive contamination will be developed and tested in this phase.

» design and production of a low-background gamma spectroscopy system attached to a chemical concentration system (SPEC) that will analyse the water after a triggered RTM alarm, thus providing information on the nature of the radioactive contaminant. New-generation inorganic gamma scintillation crystals will be evaluated in order to guarantee the expected sensitivity in the required timescale.

- design of compact front-end electronics based on CAEN know-how on digital pulse processing and radiation detector power supply systems.

- dedicated software for the automatic control of the prototype and analysis of raw data will be developed. It will be coupled to a suitable ICT infrastructure for collecting information from all monitoring nodes scattered along the tap water plant, allowing complete supervisory control via a remote web interface. The operator will be alerted in case of alarm from any of the nodes and will be able to inspect and configure each node.

The second phase of the project foresees integration of the previous tasks' results, a complete characterization test of the prototype at the Italian National Institute of Ionizing Radiation Metrology of ENEA and final installation and demonstration phase at the Warsaw Waterwork Company site.

Expected results

Improve drinking water security against deliberate or accidental radiological or nuclear threats via a new real-time alpha and beta radioactivity monitor system installed at water treatment plants.

Improve water plants' protection by offering the possibility of quickly blocking water flow at intake points in case of strong radioactive contamination.

PARTNERS	COUNTRY
Università degli Studi di Padova (UNIPD)	Italy
Costruzioni Apparecchiature Elettroniche Nucleari C.A.E.N. SpA (CAEN)	Italy
SCIONIX Hollande BV (SCIONIX)	The Netherlands
Narodowe Centrum Badan Jadrowych (NCBJ)	Poland
Agenzia Nazionale per le Nuove Tecnologie, l'Energia e lo Sviluppo Economico Sostenibile (ENEA)	Italy
Miejskie Przedsiebiorstwo Wodociagow i Kanalizacji w M. St. Warszawie Spolka Akcyjna (MPWIK)	Poland
Università di Pisa (UNIPI)	Italy
Wardynski i Wspolnicy SPK (WIW)	Poland

TWOBIAS / Two stage rapid biological surveillance and alarm system for airborne threats

© il-fede - Fotolia.com

Information

Grant Agreement N°
242297
Total Cost
€4,935,083.65
EU Contribution
€3,577,834
Starting Date
01/07/2010
Duration
36 months

Coordinator

NORWEGIAN DEFENCE RESEARCH ESTABLISHMENT
Norway
Contact
Janet Martha Blatny
Tel.: +47 63807827
Fax: +47 63807509

Project objectives

The project aim is to develop a demonstrable, modular and “close-to-market” demonstrator of a stationary, reliable, vehicle-portable, low false alarm rate Two Stage Rapid Biological Surveillance and Alarm System for Airborne Threats (TWOBIAS) for use at indoor or outdoor public sites regarded as targets for bioterrorist attacks.

The objectives are to:

» Establish a command and control software system for TWOBIAS in order to reliably function at a real-life site;

» Test and evaluate biodetectors in large-scale chamber tests, and analyse background interference detection signals under real-life conditions;

» Enhance the performance of TWOBIAS using advanced data classification methods;

» Provide a functional combined two stage alarm biological detection and identification system.

Description of the work

TWOBIAS includes both detection (BDU – biological detection unit) and identification (BIU – biological identification unit) schemes:

» *StageONE:* First alarm based on best-in-use optimized optical BDU (detect-to-warn);

» *StageTWO:* Second alarm based on highly automated microfluidic-based platform with a molecular BIU (detect-to-treat).

The project, containing six workpackages, will enhance the progress of the state-of-art technology by developing a reliable biological surveillance system TWOBIAS in order to reduce the total time response for first responders by focusing on:

» assessing the requirements from users;

» reducing false alarm rates by improving current BDUs using complementary orthogonal detector techniques obtaining classification of biological threat agents during detection;

» developing improved alarm algorithms for existing mature and almost mature BDUs;

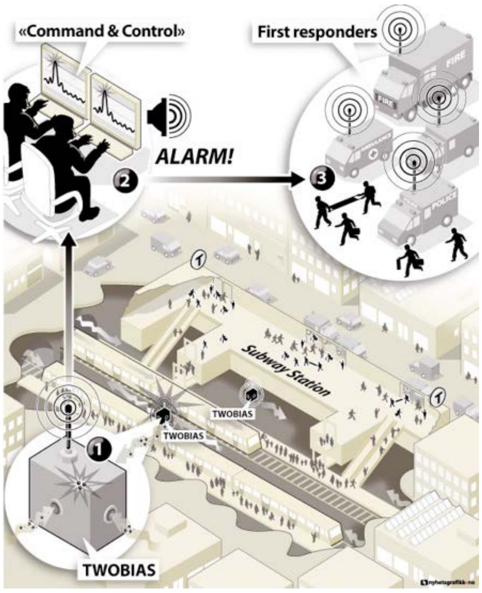
» combining the improved BDU with a semi-automatic, microfluidic, on-site, molecular identification unit (BIU) for multiplex identification of biological threat agents in the air;

» integrating the optimized BDU and BIU to obtain a demonstrator of TWOBIAS; and

» using real-life conditions for characterising, improving BDU and performing testing and evaluation of TWOBIAS together with users.

Expected results

- An integrated BDU and BIU system with a two-stage alarm functionality - TWOBIAS;
- The best-in-use BDU components with accompanying alarm algorithms (StageONE alarm);
- A reliable BIU component – automatic - microfluidic - molecular (after StageONE alarm);
- No (extremely low) false alarm rates;
- A simulation/model of the real-life test site and BDU/ TWOBIAS;
- A demonstration of TWOBIAS at a real-life test.



© Twobias

PARTNERS	COUNTRY
Norwegian Defence Research Establishment (FFI)	Norway
Centre d’Etudes du Bouchet (DGA)	France
Dycor Global Solutions Ltd (DGS)	Cyprus
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Q-linea AB (QL)	Sweden
Státní ústav jaderné, chemické a biologické ochrany, v. v. i. (SCB)	Czech Republic
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Thales SA (TRT)	France
Thales Security Solutions and Services S.A.S (TSS)	France
Uppsala universitet (UoU)	Sweden

AVERT / The Autonomous Vehicle Emergency Recovery Tool (AVERT) provides a capability rapidly to deploy, extract and remove both blocking and suspect vehicles from vulnerable positions and confined spaces.

© Arindam Banerjee - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285092
Total Cost
€3,685,613.65
EU Contribution
€2,810,822
Starting Date
01/01/2012
End Date
31/03/2015

Coordinator

IDUS Consultancy Ltd
10 Lime Close
RG41 4AW, Wokingham,
United Kingdom
Contact
Richard James May
Tel: +44 118 979 1828
Mobile: +44 77 333 20856
E-mail: Richard.may@idusconsultancy.co.uk
Website: www.avertproject.eu/

Project objectives

Terrorism can lead to horrific loss of life, extensive disruption to city transport and damage to commercial real estate. Vehicles provide an ideal delivery mechanism because they can be meticulously prepared well in advance of deployment and then brought in to the Area of Operations. Furthermore, a real and present danger comes from the threat of Chemical, Radiological, Biological and Nuclear (CRBN) contamination.

Current methods of bomb disruption and neutralisation are hindered in the event that the device is shielded, blocked or for whatever reason cannot be accessed for examination.

The Autonomous Vehicle Emergency Recovery Tool (AVERT) provided a unique capability to Police and Armed Services to rapidly deploy, extract and remove blocking vehicles from vulnerable positions such as enclosed infrastructure spaces, tunnels, low bridges as well as under-building and underground car parks. This then allowed access for Explosive Ordnance Disposal (EOD) operation.

Description of the work

The project covered the development and demonstration of a proof of concept for an Autonomous Vehicle Emergency Recovery Tool (AVERT). This was designed to assist EOD teams by locking onto the vehicle(s) which is (are) obstructing the deployment of EOD systems and rapidly and safely removing it (them) from the path to allow speedier access than can currently be achieved.

The AVERT project concept is to automate the placing of lifting bogies, capable of omnidirectional movement, under the road wheels of identified vehicles and to synchronise their lifting and path as a group in order to remove the vehicle without disturbance. Vehicles can be removed from confined spaces (e.g. where the height level is constrained) with delicate handling, swiftly and in any direction to a safer disposal point to reduce or eliminate collateral damage to infrastructure and personnel.

The operational framework was targeted at a system which was deployed alongside EOD robots and equipment. This system comprised a number of independent lifting bogies, one for each wheel of the blocking vehicle to be moved. The bogies were deployed from a carrier platform (Deployment Unit) and each locked onto a road wheel on the designated vehicle. Once in position, the swarm of bogies acted in synchronisation to raise the road wheels and move the vehicle along a safe path, allowing the existing EOD robot access for neutralising operations.

The concept also included a Command Console which is detached from the Deployment Unit and held at the command post. This console was designed to provide the commander with command and executive control of the operation by designating the desired access path and confirming the sequence of vehicles to be moved to achieve it.

AVERT was commanded remotely and operated autonomously under its own power and sensor awareness, as a critical tool alongside existing technologies, thereby enhancing bomb disposal response speed and safety.

Results

The Autonomous Vehicle Emergency Recovery Tool (AVERT) started in 2012 as a research project to provide a unique capability to Police and Armed Services and for Improvised Explosive Device Disposal teams in dealing with suspect vehicles.

AVERT can provide an autonomous capability to deploy, extract and remove blocking or suspect vehicles from vulnerable positions such as enclosed infrastructure spaces, tunnels or low bridges.

Vehicles can be removed from confined spaces with delicate handling, swiftly, and in any direction to a safer disposal point to reduce or eliminate collateral damage to infrastructure and personnel. Remote operation, self-powered and onboard sensors provides a new capability that can operate alongside existing technologies, thereby enhancing bomb disposal response, speed and safety. AVERT can operate autonomously but with a man-in-the-loop control.

AVERT was successfully demonstrated in March 2015. It has received positive feedback and strong interest from end user nations and industrial partners. It is expected that AVERT could enter production in 2016.

This project could have a high impact for safeguarding the security of citizens in the face of terrorist attacks.

PARTNERS	COUNTRY
IDUS Consultancy Ltd (IDUS)	United Kingdom
BB-Ingenieure Ingenieurbüro (BBI)	Germany
Zurcher Hochschule Fur Angewandte Wissenschaften (ZHAW)	Switzerland
Democritus University of Thrace (DUTH)	Greece
Marshall System Design Group Ltd (MSDG)	United Kingdom
Force Ware GmbH (FW)	Germany

BONAS / BOmb factory detection by Networks of Advanced Sensors

© Robert Reich – istockphoto.com

Information

Grant Agreement N°
261685
Total Cost
€4,971,631.81
EU Contribution
€3,488,360.01
Starting Date
01/04/2011
Duration
42 months

Coordinator

AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE
Diagnostics and Metrology Laboratory (UTAPRAD-DIM)
Via Enrico Fermi 45
00044 Frascati, Rome
Italy
Contact
Antonio Palucci
Tel: +390694005299
Mobile: +393298313933
Fax: +390694005334
E-mail: antonio.palucci@enea.it
Website: www.bonas-fp7.eu

Project objectives

The BONAS project presents the following objectives:

» To design, develop and test a novel wireless sensor network for increasing citizen protection and homeland security against threats posed by IED devices. The sensor network will focus on the detection of traces of precursors used in IED production (particulates, gases, waterborne) in the vicinity of a "bomb factory". This will contribute to the determination of the "factory's location", allowing an early threat thwart.

» To perform a feasibility study that will assess the usefulness and potential advantages that the BONAS concept will bring about in the future. A cost analysis will be performed in order to foresee the financial effort associated with the field deployment of such a sensor network, its operation and maintenance.

» To demonstrate the BONAS concept in a close to real-life scenario, implementing all developed network sensors with the aim of evaluating their performance and larger scale deployment potentials.

» To investigate and prepare the potential future deployment of key sensors aboard a flying platform with a view towards increasing the BONAS network detection capabilities.

Description of the work

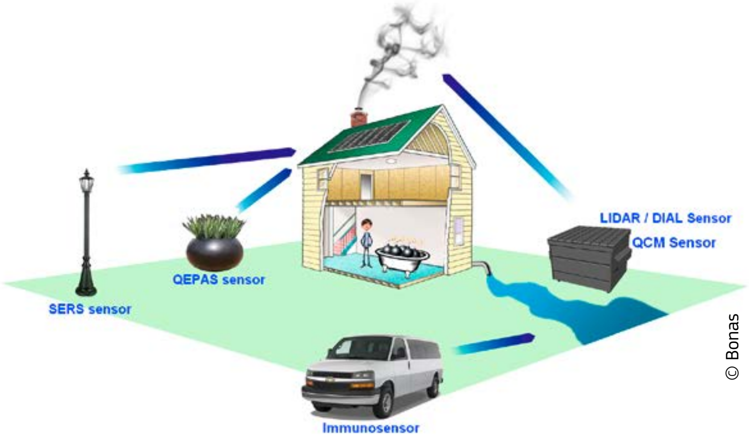
The aim of BONAS is to design, develop and test a novel wireless sensor network for increasing citizen protection and homeland security against terrorist attacks, in particular against the threat posed by IED devices. The sensor network will focus on the detection of traces of precursors used in IED production (particulates, gases and/or waterborne) present in the environment surrounding the vicinity of a "bomb factory". The different sensors are specifically designed to be deployed in sensitive locations and easily camouflaged. This network will help pinpoint the "factory's location", allowing an early threat thwart. A feasibility study will assess the usefulness and potential advantages that the BONAS concept will bring about in the future and the costs of mass production of sensor networks integrating COTS components.

BONAS intends also to investigate and prepare the potential future deployment of key sensors aboard a flying platform with a view towards increasing the BONAS network detection capabilities. The wireless sensor network will feature a variety of sensing devices (in-situ and remote), that will jointly provide broad chemical spread and low false alarm rates through an expert system management of the data collected. In particular, BONAS will develop a Lidar/Dial system; QEPAS sensor; SERS sensor; QCM sensor; and electrochemical sensor.

BONAS includes a multidisciplinary team of leading European research groups together with industrial organizations and end-users with previous experience and activity in the field of specific local and remote sensor development and with experience on security projects. The consortium represents the complete supply chain of the proposed product, which sets good perspectives for exploitation and commercialization of the generated innovations. The consortium will be supported by an already established Advisory Board formed by experts from the various police corps.

Expected results

The BONAS project envisages an innovative, large-scale sensor network in the future, able to detect IED preparation with a minimum rate of false alarms and relying on three different layers. The target substances will comprise explosive and precursor substances contained in IEDs. The concept is based on a series of increasingly specific tests taking place in increasingly smaller areas starting with general tests and then reducing the search area. Each one of the referred layers will correspond to a different phase of threat detection and to different levels of the wireless sensor network.

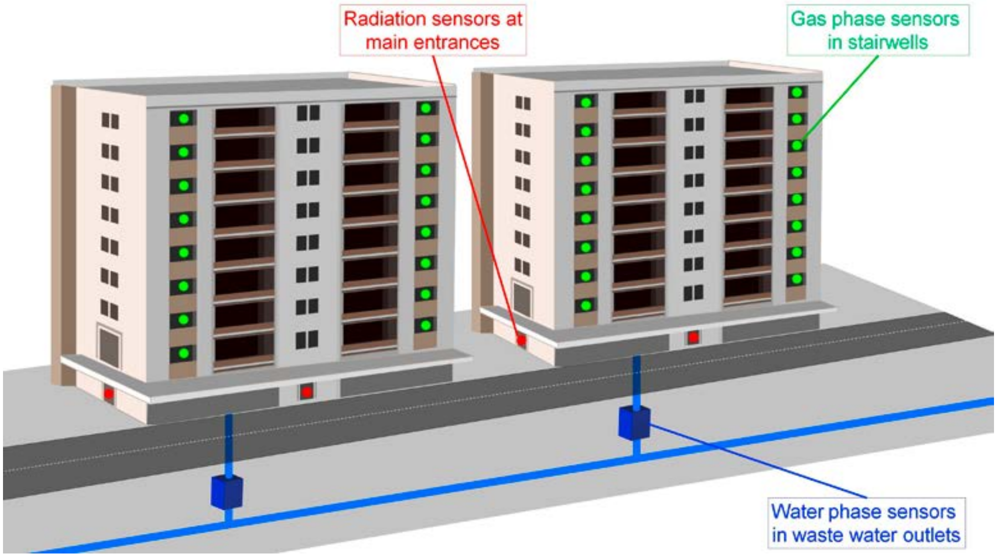


© Bonas

PARTNERS	COUNTRY
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE (ENEA)	Italy
CONSORZIO CREO-CENTRO RICERCHE ELETTRO OTTICHE (CREO)	Italy
SERSTECH AB (SAB)	Sweden
TEKEVER – TECNOLOGIAS DE INFORMACAO, S.A. (TEK)	Portugal
LASER DIAGNOSTIC INSTRUMENTS AS (LDI)	Estonia
CSEM CENTRE SUISSE D'ELECTRONIQUE ET DE MICROTECHNIQUE SA - RECHERCHE ET DEVELOPPEMENT (CSEM)	Switzerland
EADS DEUTSCHLAND GMBH (EADS)	Germany
UNIVERSITE CLAUDE BERNARD LYON 1 (UCBL)	France
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONE)	France
UNIVERSITE DE LAUSANNE (UNIL)	Switzerland
NATIONAL BUREAU OF INVESTIGATION (NBI)	Finland
KING'S COLLEGE LONDON (KCL)	United Kingdom
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)	France
QUEEN'S UNIVERSITY BELFAST (QUB)	United Kingdom

COMMONSENSE / Development of a Common Sensor Platform for the Detection of IED “Bomb Factories”

© Created by Hugh Doyle, Tyndall National Insitute, 2011


Radiation sensors at main entrances
Gas phase sensors in stairwells
Water phase sensors in waste water outlets

Information

Grant Agreement N°
261809
Total Cost
€4,768,992
EU Contribution
€3,404,935
Starting Date
01/01/2011
Duration
36 months

Coordinator

UNIVERSITY COLLEGE CORK, NATIONAL UNIVERSITY OF IRELAND
Tyndall National Institute
Western Road
Cork
Ireland
Contact
Hugh Doyle
Tel: +353 (0)21 490 4177
Fax: +353 (0)21 490 4058
E-mail: info@fp7project-commonsense.eu
Website: www.fp7project-commonsense.eu

Project objectives

The detection of chemical explosives is crucial for homeland security, environmental cleaning, and humanitarian efforts. Chemical explosives encompass a variety of compounds, with different vapour pressures, solubilities and chemical reactivities, making broad-class detection a serious challenge. While many sensing methods currently exist, none is ideal. Principal deficiencies include lack of portability, a susceptibility to false positive results due to environmental contaminants or false negative results to interfering compounds. The need exists for a single distributed network, with a common interface and communications protocol, to manage and communicate with a variety of different sensor technologies, and use the combined sensor data to produce clear results with low false positive/negative readings. The objective of the CommonSense project is to create and demonstrate such a single distributed network, with common interface and communications protocols, to manage and communicate with a variety of different sensor technologies, and to use the combined sensor data to produce clear results with low false positive/negative readings.

Description of the work

The work plan for the CommonSense project is divided into five complementary technical work packages:

Design and Specification
At the start of the project, the partners will specify target IED analytes, detection limits and test conditions relevant to end users. Specification of the common testing and benchmarking procedures, operating protocols, network architectures and communications protocols will also be carried out.

Materials Development and Characterisation
A variety of novel molecular, polymeric and nanostructured sensor materials will be developed and characterised with respect to their optoelectrical and photophysical properties, especially their response to sub-ppb (gas phase) and sub-ppm (liquid) levels of explosive compounds.

Sensor Development
Development of the sensor modules will be carried out at separate partner sites for initial testing and characterisation. A variety of different electrical, opto-electrical and opto-electrochemical devices for gas- and water-phase detection of IED analytes will be developed. A series of radiation detection modules will also be developed.

Software Development and Networking
Development of the common network platform for control and communication of the sensor modules. Driver software for control and read-out from different sensor types will be done at partner sites prior to integration with the network and the chemometric “learning” algorithms.

Integration, Testing and Industrial Validation
Integration of the sensor modules and quantitative testing and validation of the performance of the sensor modules. The final testing and assessment will be carried out in a “real-world” environment.

These are supported by two non-technical work packages focusing on dissemination & exploitation of project results and project management.

Expected results

The expected results from the project are:

- » Development of modules for gas-phase detection of explosives with ppb sensitivity;
- » Development of modules for water-phase detection of explosives with sub-ppm sensitivity;
- » Development of a small form factor low-power gamma radiation sensor with <10% energy resolution and an energy range of 60keV to 2MeV;
- » Development of an intelligent learning network, using chemometric algorithms to teach itself to detect explosives and ignore interferents.

PARTNERS	COUNTRY
University College Cork, National University of Ireland (UCC)	Ireland
Israel Institute Of Technology (Technion)	Israel
The University Of Manchester (UNIMAN)	United Kingdom
Alphasense Limited (ALPHA)	United Kingdom
Bundesanstalt Fuer Materialforschung und Pruefung (BAM)	Germany
SensL Technologies Limited (SENSL)	Ireland
Thales Communications S.A. (TCF)	France
Police Service of Northern Ireland (PSNI)	United Kingdom

D-BOX / Comprehensive toolbox for humanitarian clearing of large civil areas from anti-personal landmines and cluster munitions

Information

Grant Agreement N°
284996
Total Cost
€9,909,587.90
EU Contribution
€6,898,085.95
Starting Date
01/01/2013
Duration
36 months

Coordinator

Astrium SAS (ASTRIUM)
ASTRIUM SPACE TRANSPORTATION
51-61 route de Verneuil
PO Box 3002
78133 Les Mureaux
France
Contact
Bruno Esmiller
Tel: +33 1 39 06 29 66
Mobile: +33 6 15 18 39 97
Fax: + 33 1 39 06 14 40
E-mail: bruno.esmiller@astrium.eads.net
Website:
www.d-boxproject.eu

Project objectives

Landmines and cluster munitions continue to kill or maim civilians every day in countries all around the world, even long after conflicts are over. Assuming no additional mines are laid from now on, at the current rate of clearance of some 500,000 mines per year it could still take hundreds of years to find and clear all the landmines around the world.

D-BOX will tackle this burning issue of anti-personal landmines and cluster munitions inherited from armed conflicts. This will be achieved through the development of innovative solutions that will be interfaced and integrated in a comprehensive toolbox to provide demining stakeholders with the best tools, methods and procedures for:

» Mapping and localization (long distance) of hazardous areas

» Close-in detection (short distance)

» Risk management

» Human, ethical and legal factors (including procedures and best practices)

» Neutralization of anti-personal landmines and cluster munitions in an open and civil environment,

» Protective equipment for operators and population

» Training solutions for personnel

This "smart" toolbox could be used during all demining activities (from the mission's preparation to the elimination of mines, including communication to general public and donors). It could also help operators and end users get the most suitable answers to technical problems and, finally, find the lowest cost and "easy to use" tools for specific tasks during demining activities that are adapted to different scenarios and conditions.

D-BOX Toolbox will help them choose the most suitable solutions, taking into account the environment (terrain, vegetation, age of mines, local population, culture, etc.) and thus enabling an optimization of operations in the field faster demining and a lower cost per square meter.

Description of the work

The development of D-BOX is mainly based on the assessment of past and ongoing activities and legacy tools. Completion of the project concept will lead to development of the actual D-BOX Toolbox. Before populating the latter with real functions (tools and procedures), an advanced information system will be developed to organize the Toolbox. This will provide an easily understandable user interface for access to all functions in the Toolbox, where data collection will be very important.

In parallel, innovative tools, methods and procedures will be developed or improved in the following domains: human, ethical and legal factors, mapping and localization of hazard zone, close-in detection, neutralization in a civil environment, protective equipment for personnel and population, training solutions and mine risks population education.

The Toolbox's components will be carefully tested tool by tool, by function and as groups of functions. Finally, an assembled complete version of the integrated Toolbox will be subject to full scale field validation via different relevant demining scenarios.

End users and stakeholders will provide their experience and requirements during the whole process from concept design, Toolbox development, development of information and training kit to the Toolbox's testing and validation.

When needed, the industrial stakeholder platform will be called upon to carry out integration, modifications and development of technology.

Expected results

The D-BOX Toolbox will significantly increase the humanitarian demining capability. It will be modular and upgradable, and its deployment will be adapted to each situation and user.

It will provide various toolboxes with different complexity and completion to be used in different places by a variety of users. Furthermore, the D-BOX solution will improve significantly demining productivity and safety by increasing the current rate of clearance and cost-effectiveness. It will also allow for more effective application of solutions that encompass simple and advanced technologies.

The D-BOX Toolbox will meet the most recent needs of demining stakeholders: mapping of hazard zone and close-in detection with low cost and easy to use tools.

The D-BOX Toolbox will tackle the main challenges for the development of new de-mining technologies:

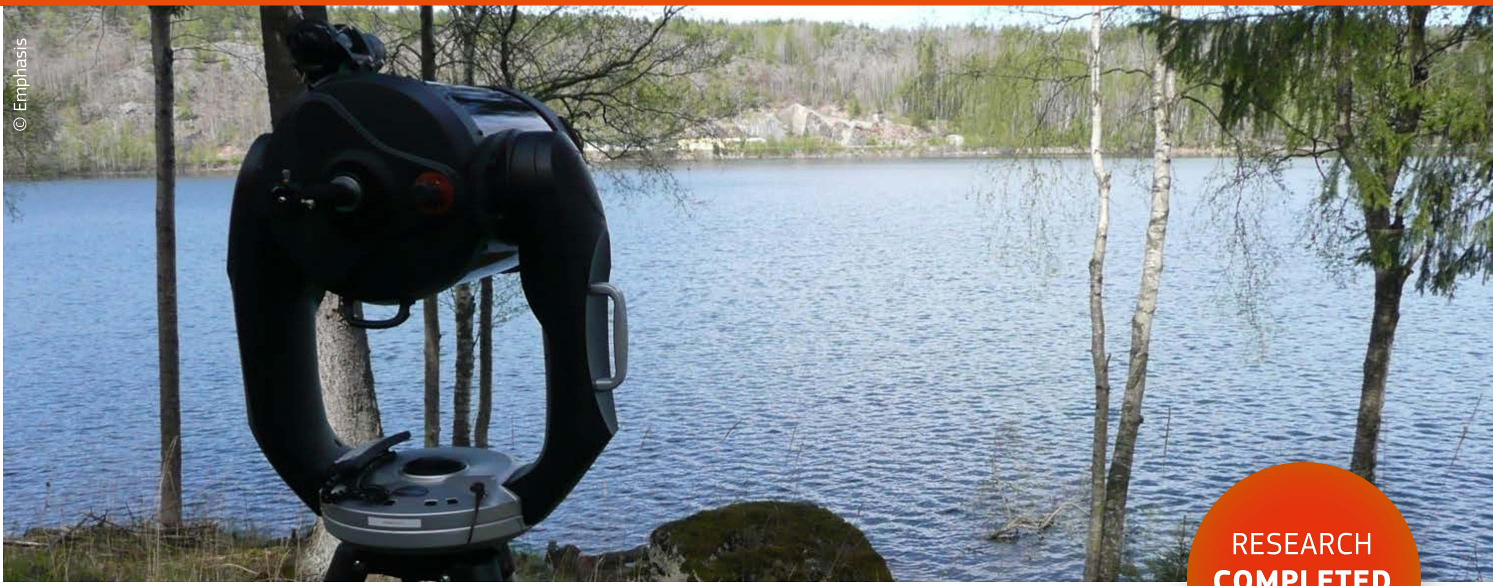
» the tremendous diversity of environmental conditions in which landmines are employed and the variety of these mines and cluster munitions

» different training levels, cultural backgrounds, and educational levels of deminers

» detection of mines made with plastic and low metal content, while at the same time discriminating them from non-explosive debris.

PARTNERS	COUNTRY
Astrium SAS (ASTRIUM)	France
Astri Polska Spolka z ograniczona odopowiedzialnoscia (APL)	Poland
Bactec International Limited (BACTEC)	United Kingdom
CBRNE Limited (CBRNE)	United Kingom
Comite Europeen de Normalisation (CEN)	Belgium
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Italy
Technische Universiteit Defft (TUD)	The Netherlands
Totalforsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V (FRAUNHOFER)	Germany
Infoterra Limited (INFOTERRA)	United Kingdom
Instytut Technologii Bezpieczeństwa MORATEX (MORATEX)	Poland
Consorzio Universita Industria – Laboratoria di Radiocomunicazioni RADIOLABS (RADIOLABS)	Italy
Selex ES S.P.A. (SELEX)	Italy
TerraSpatium SA (TERRASPATIUM)	Greece
Telespazio SPA (TELESPAZIO)	Italy
Netherlands Organisation for Applied Scientific Research (TNO)	The Netherlands
Univeristy of Surrey (SUR)	United Kingdom
Teknologian Tutkimuskeskus VTT (VTT)	Finland
University of Leicester (ULEIC)	United Kingdom
e-GEOS S.p.A. (E-GEOS)	Italy

EMPHASIS / Explosives Material Production (Hidden) Agile Search and Intelligence System


© Emphasis

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261381
Total Cost
€4,593,272.90
EU Contribution
€3,406,050.72
Starting Date
01/10/2011
End Date
31/01/2015

Coordinator

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Department: Defence & Security, Systems and Technology Unit: Weapon Effects and Security of Explosives
Gullfossgatan 6
SE-164 90, Stockholm, Sweden
Contact
Swedish Defence Research Agency
Tel: +46 8 5550 3000
Fax: +46 8 5550 3949
E-mail: registrator@foi.se
Website: www.emphasis-fp7.eu

Project objectives

EMPHASIS project tested a surveillance system concept for detecting and localising the illicit production of explosives and improvised explosive devices (IEDs) in urban areas. Its system is composed of networked sensors. Area detectors to monitor explosives or their precursors in the vapour phase were used, as were multiple static sensors positioned in sewers to monitor the latter for indicative traces.

All the data about a detected threat substance – its type, location, time and amount – was fused and evaluated at a command centre where appropriate action could be taken. The project's strategy was to divide a large area into smaller segments with more sensors to localise a bomb factory, with the latter's exact pinpointing carried out by stand-off detectors in mobile equipped units.

Description of the work

EMPHASIS offered a novel way to perform surveillance across a very large area to detect explosives and their precursors and IEDs. A key aspect of its concept was to enable efficient intelligence-led assessment of a targeted urban area to establish where and when illicit bomb-making activity was taking place.

The project's area-monitoring sensors cover hundreds of meters and thus a large area of coverage. Moreover, its stand-off sensors can detect explosives traces that have been transferred to surfaces by the perpetrators who handled the explosives. Combining this with ion selective electrodes capable of detecting precursors/explosives in the sewage makes for an extensive system of detection.

A feasibility and cost effectiveness study was done to assess the system's potential for commercialisation.

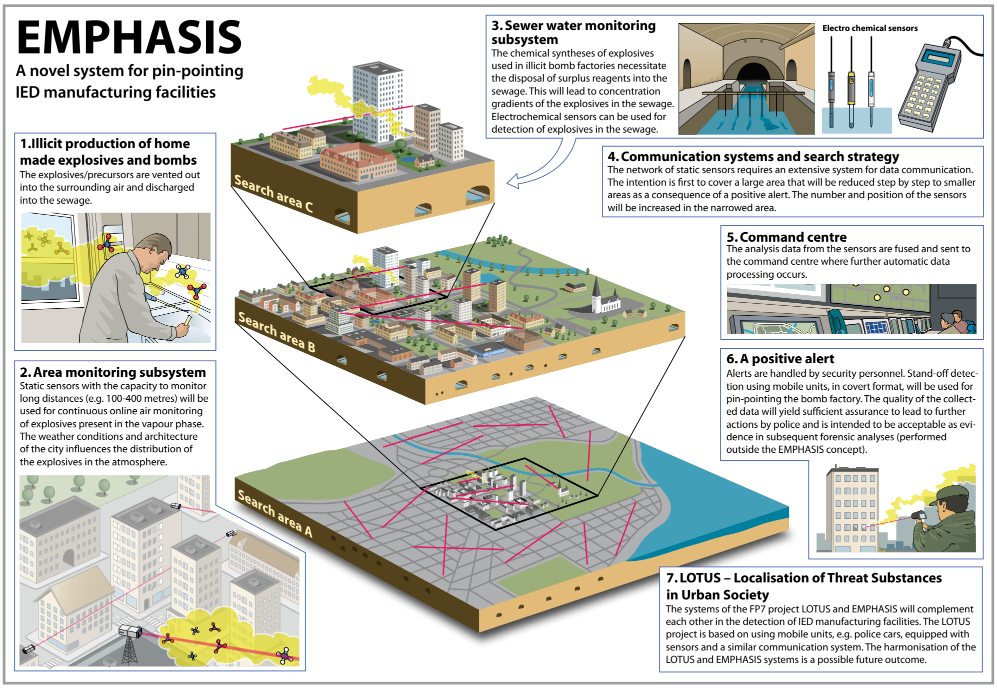
A successful system based on EMPHASIS's technology could lead to a very significant reduction in surveillance man-power in suspect areas. And it would support the timing of police intervention, leading to a higher conviction rate.

Results

A key advantage of EMPHASIS's system is its complementarity with technologies developed by LOTUS, another FP7 project. The latter's data and developments were implemented as much as possible, e.g. exploitation of knowledge about central command, threat substance lists, dispersion and modelling of threat substances in the air and in LOTUS's home explosive laboratory.

EMPHASIS' detection effort focused on three types of cases: i) detection of explosives/precursors in vapour phase at low concentrations; ii) detection of explosives/precursors at low concentrations in sewage; and iii) detection of particles (low concentrations) on door-handles or other covered surfaces. The fusion of such sensor data leads to potential alerts.

On 7 July 2005, four bombs exploded within a short time on three of London's metro trains and one of its double-decker buses. The homemade bombs were packed into rucksacks whose discovery by traditional intelligence and police work was difficult. An EMPHASIS system would help discover illicit activities at an early stage, making neutralization easier and with far fewer consequences. This would be one of the positive impacts of the project.



EMPHASIS

A novel system for pin-pointing IED manufacturing facilities

1. Illicit production of home made explosives and bombs
The explosives/precursors are vented out into the surrounding air and discharged into the sewage.

2. Area monitoring subsystem
Static sensors with the capacity to monitor long distances (e.g. 100-400 metres) will be used for continuous online air monitoring of explosives present in the vapour phase. The weather conditions and architecture of the city influences the distribution of the explosives in the atmosphere.

3. Sewer water monitoring subsystem
The chemical syntheses of explosives used in illicit bomb factories necessitate the disposal of surplus reagents into the sewage. This will lead to concentration gradients of the explosives in the sewage. Electrochemical sensors can be used for detection of explosives in the sewage.

4. Communication systems and search strategy
The network of static sensors requires an extensive system for data communication. The intention is first to cover a large area that will be reduced step by step to smaller areas as a consequence of a positive alert. The number and position of the sensors will be increased in the narrowed area.

5. Command centre
The analysis data from the sensors are fused and sent to the command centre where further automatic data processing occurs.

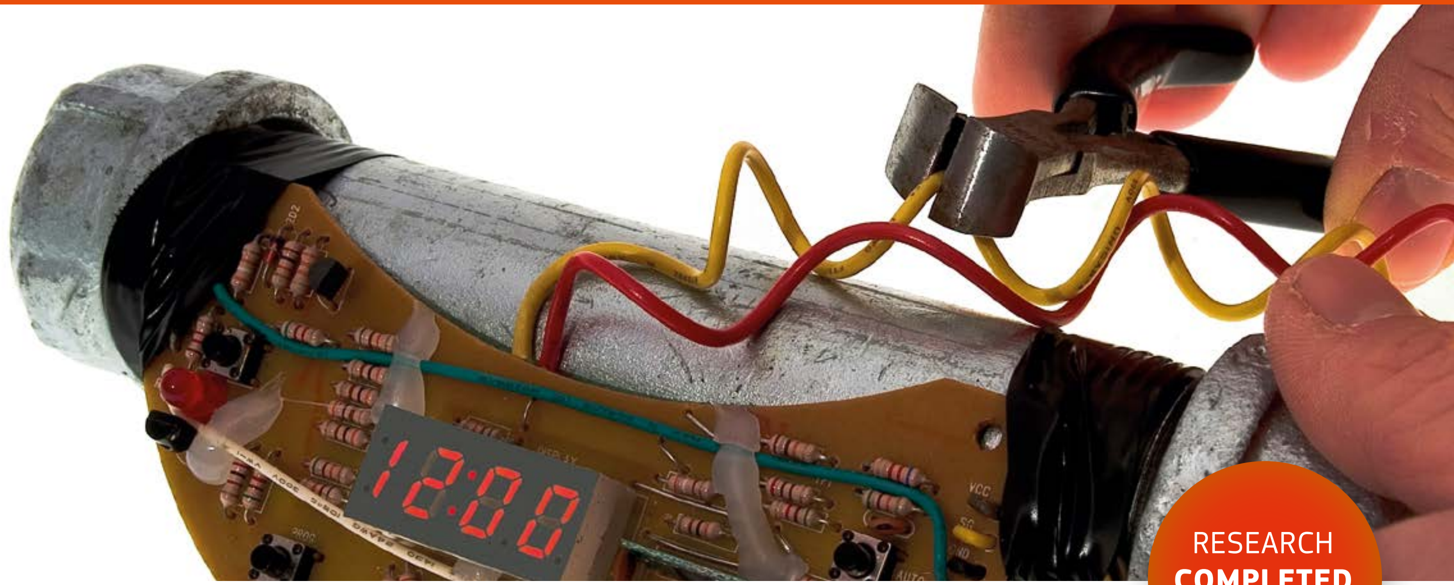
6. A positive alert
Alerts are handled by security personnel. Stand-off detection using mobile units, in covert format, will be used for pin-pointing the bomb factory. The quality of the collected data will yield sufficient assurance to lead to further actions by police and is intended to be acceptable as evidence in subsequent forensic analyses (performed outside the EMPHASIS concept).

7. LOTUS – Localisation of Threat Substances in Urban Society
The systems of the FP7 project LOTUS and EMPHASIS will complement each other in the detection of IED manufacturing facilities. The LOTUS project is based on using mobile units, e.g. police cars, equipped with sensors and a similar communication system. The harmonisation of the LOTUS and EMPHASIS systems is a possible future outcome.

© Emphasis

PARTNERS	COUNTRY
Totalförsvarets forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT-IAF)	Germany
PORTENDO AB (Portendo)	Sweden
Cascade Technologies Limited (Cascade)	United Kingdom
Morpho (MPH)	France
Institut National de Police Scientifique (INPS)	France
VIGO SYSTEM S.A. (VIGO)	Poland

ENCOUNTER / Explosive Neutralisation and Mitigation Countermeasures for IEDs in Urban/Civil Environment



© istockphoto

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285505
Total Cost
€4,412,123
EU Contribution
€3,313,630
Starting Date
01/05/2012
End Date
31/08/2015

Coordinator

SWEDISH DEFENCE RESEARCH AGENCY (FOI)
Department of Physical Protection and Weapons Effects
Grindsjön Research Centre
SE-14725 Tumba, Sweden
Contact
Pernilla Magnusson
Tel: +46-8 5550 3939
Mobile: +46 709277209
Fax: +46 855504180
E-mail:
pernilla.magnusson@foi.se
encounter@foi.se
Website:
http://www.encounter-fp7.eu

Project objectives

The ENCOUNTER project will consider threats from Improvised Explosive Devices (IED) in the urban environment. The project objectives are to:

» Increase urban security through improved procedures for dealing with an IED.

» Prevent IED explosion after discovery through new technologies for their neutralisation. This would mean most people need never be aware an IED was present, reducing the impact of the IED in achieving the terrorists' aims.

» Drastically reduce damage if the IED is triggered, through development of explosion-mitigating and fragment-prevention technologies. This will enable the urban environment to 'bounce-back' to normal life as quickly as possible.

» Consider the ethical, societal and financial aspects of new ways to dealing with IEDs to ensure the response is in proportion to the threats, and that the response does not create any additional problems.

In summary, the ENCOUNTER project will identify, explore and validate existing and innovative techniques for mitigation and neutralisation of already discovered IEDs in the urban/civil environment. The results will be summarised in a recommendation matrix and used to develop a software tool to assist clearing forces.

Description of the work

The concept of the ENCOUNTER project is based on:

Review of practices and state of the art.

This part deals with the operational and technical aspects associated with the neutralisation of IEDs and the actions and means that mitigate the damage they will cause if detonated:

» Review of the practices, policies and procedures of the police and security units responsible for Explosive Ordnance Disposal (EOD).

» State of the art review of the existing technologies for neutralisation of IEDs and the means and tools for the mitigation of damage.

» Identification of scenarios and design basis threats for the work packages focusing on R&D and on the examination and evaluation of technologies.

Development of technological capacities in two areas:

» Development and assessment of IED neutralisation technologies and assessment of EOD response bodies' practices.

» Development and assessment of damage mitigation means and decision support tools for EOD response bodies.

Ethical and societal aspects.

Consider the ethical, societal and financial aspects of new ways to deal with IEDs to ensure the response is in proportion to the threat, and that the response does not create any additional problems. This will:

» Give stakeholders guidelines for evaluating and improving acceptance of IED neutralisation techniques

- » Reduce worries of citizens regarding the application of IED neutralisation
- » Understand how techniques are perceived and which techniques have a positive impact on the population's perception of security
- » Cost-benefit assessment of the technologies used for IED mitigation and neutralisation

Experiments, tests and evaluation.

Review, tests and evaluation of the range of means, tools and practices that will be developed within the framework of the project's R&D work packages. This includes tests of neutralisation technologies and IED damage mitigation experiments in the laboratory and field conditions, with the use of live IEDs.

Results

The project outcome will describe the practices, tools and procedures for neutralising (N) or mitigating (M) the effects of IEDs and how to respond appropriately and effectively to the threat they present in the urban environment. The N/M technologies will be assessed in relation to the threat and their effectiveness in dealing with the various scenarios that EOD bodies and police units address.

The capability to review and evaluate the various technologies in relation to the concept of operation (CONOP) of the EOD bodies and the police units operating in the urban environment will be developed.

PARTNERS	COUNTRY
Totalförsvarets forskningsinstitut (FOI)	Sweden
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung E.V (EMI)	Germany
The University of Sheffield (USFD)	United Kingdom
Ingeneria de Sistemas Para La Defensa de Espana SA (ISD)	Spain
Tamar Israeli Advanced Quarrying Co Ltd (TMR)	Israel
Albert-Ludwigs-Universität Freiburg (ALU-FR)	Germany
Blastech Ltd (BLT)	United Kingdom

EXPEDIA / Explosives PrEcursor Defeat by Inhibitor Additives

Information

Grant Agreement N°
604987
Total Cost
€4,428,539.50
EU Contribution
€3,480,602.00
Starting Date
01/09/2014
Duration
36 months

Coordinator

TOTALFÖRSVARETS FORSKNINGSINSTITUT (FOI)
Totalförsvarets forskningsinstitut (FOI)
Defence and Security, Systems and Technology
Gullfossgatan 6
SE-164 90 Stockholm,
Sweden
Contact
Totalförsvarets forskningsinstitut
Tel: +46 8 5550 3000
Fax: +46 (0)8 5550 3949
E-mail: registrator@foi.se
Website:
www.expedia-fp7.eu

Project objectives

Home-grown terrorism is increasing in Europe and elsewhere in the world. The bombings in Paris 2015, Boston 2013, Oslo 2011, Stockholm 2010 and London 2004 are just a few examples where home-made explosives (HME) were used in terror attacks.

There are a vast number of different chemicals that could be turned into dangerous HME, given the right chemical knowledge and equipment. EXPEDIA will aim find chemical solutions to prevent the misuse of certain explosive precursors and to increase knowledge about *garage chemistry*. It will collect information to gain a better understanding of how terrorists create HME, the chemicals they use and where they find them on the open market. The project will study how easily HME can be created, the basic equipment needed and the chemical knowledge required of the terrorist. The knowledge gleaned about HME will serve as input to define *a European guide for first responders* -- one of the outcomes that EXPEDIA will produce.

Description of the work

In principle there are four ways to eliminate or reduce the threat from HME:

1. Obstruct the supply chain of explosive precursors

2. Prevent the illegal production of initiator systems

3. Use chemicals to inhibit the main charges

4. Carry out early detection of bomb factories

Improvised manufacturing of explosives is easily carried out, but it is more difficult to ensure that the explosives work as intended. EXPEDIA will evaluate what terrorists can do with precursors via the materials that are still available to the general public.

EXPEDIA will add chemical inhibitors to frequently used explosive precursors used in initiator systems and main charges. These inhibitors will prevent or make it much more difficult to use the explosive precursor in the synthesis and formulation of HMEs.

The threat from bomb attacks within Europe needs to be counter-measured on a European level. EXPEDIA will deliver *a European guide for first responders* with information about the hazards and safe handling of such materials.

Finally, its work will feed scientifically approved facts about HME to the Commission's Standing Committee on Explosive Precursors.

Expected results

If successful inhibiting agents can be identified, it will be possible to counter terroristic attacks at an earlier stage in terrorist planning. Industries are involved in EXPEDIA's consortium due to their interest in finding viable solutions to the misuse of their products. Their participation also ensures that the project's research will focus on solutions that can be realistically implemented. EXPEDIA's work *on garage chemistry* will result in a better understanding of HME, which will help European society become more *proactive* in the fight against terrorism.

PARTNERS	COUNTRY
Totalförsvarets forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	France
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (ICT)	Germany
Yara International ASA (Yara)	Norway
Esbit Compagnie GmbH (ESBIT)	Germany
KCEM AB (KCEM)	Sweden
National Bureau of Investigation (NBI)	Finland
Wojskowy Instytut Higieny i Epidemiologii (WIHiE)	Poland
Brodarski Institute (BI)	Croatia
Bundeskriminalamt (BKA)	Germany

FORLAB / FORensic LABoratory for in-situ evidence analysis in a post blast scenario

© FORLAB

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285052
Total Cost
€4,473,920
EU Contribution
€3,087,446
Starting Date
01/03/2012
End Date
28/02/2015

Coordinator

INDRA SISTEMAS S.A
Innovation Directorate
Avenida de Bruselas 35
28108 – Alcobendas
Madrid - Spain
Contact
Francisco Javier
Hernández Crespo
Tel: +34 914 808 392
Mobile: +34 620 977 171
Fax: +34 914 806 031
E-mail: fjhernandez@indra.es
Website: www.fp7-forlab.eu

Project objectives

The FORLAB project relates to the problem of evidence collection in the post-blast scene after an IED attack. FORLAB will provide the End Users, the scientific police, with a new tool that will improve their efficiency in the investigation of the crime scene by:

» Providing fast analytical technologies to improve the evidence collection in order to reduce the number of samples to be collected and sent to the reference laboratory for detailed analysis;
» Providing a real time 3D recreation of the scene for identification of areas of the scene of higher interest and helping in the re-creation of the scene for later investigations;
» Establishing bidirectional feedback between the Command and Control Centre (where all the information about the investigation is available) and the field technicians. This will make the investigation more efficient.

FORLAB was compatible with the in-use forensic procedures and preserved the chain of custody.

Description of the work

The project activities of FORLAB have been broken down into 11 work packages and distributed in 36 months.

FORLAB developed a new concept for the investigation of the post-blast scene of an IED based attack, complementing the existing forensic procedures in use by security forces in Europe.

The research in FORLAB was focused on four main areas:

» Quick elaboration of a 3D model of the scene;
» Development of technologies for in-situ searching and screening of evidence;
» Accurate positioning of the evidence and dedicated communication network;
» Information management tools for real time exploitation of the results of the investigation.

The works were structured in four stages:

The first stage was dedicated to the System Definition with a strong involvement of End Users of the consortium. The procedures already in use by Security Forces around Europe have been reviewed and the concept of the FORLAB has been defined.

The second stage was the development of the technologies needed based on the operational requirements of the End Users.

» LIF, LIBS, Raman and NLJD were developed to improve the capability for searching and screening samples;
» A communication and positioning system was developed to meet the requirements of the investigators;
» A system for real time re-creation of the post-blast scene was developed;
» Information management tools were developed to support operations in the Command and Control Centre where all the information on the scene were available, in real time.

The third phase was the integration of a subsystem in a two-step approach: Field testing of the individual technologies was performed to obtain feedback on the achieved performance.

Finally the complete system has been validated in post-blast scenarios to verify the achieved performance. The scenarios were carefully selected with strong involvement of End Users of the project.

Partial results of the project were disseminated at public and restricted levels. Workshops with the stakeholders were organized.

Results

The main project innovation focused on establishing a dynamic, real-time feedback loop between the forensic team involved in the evidence-collection process at post-blast scenes and the distant laboratory, where all information from the scene is available in real time.

To achieve its aims, FORLAB developed a system of highly advanced analytical forensic technologies (LIBS-RAMAN, LIF, NLJD) for sample screening and 3D scenario recreation in just a few minutes. The end users taking part in the project are highly involved in optimising the system, providing a valuable tool that enables command and control centres to take real time decisions.

The project partners organised a simulated scenario (including a real explosion) and conducted laboratory tests to validate the technologies with the aim of perfecting the system.

The project is set to improve procedures used by European security forces to investigate crime scenes, particularly after blasts, by reducing the overall time needed to complete the investigation. The new integrated technology will reduce the number of laboratory samples required and support investigators in identifying the perpetrators.

The technology developed by the consortium will play a vital role in protecting society by identifying the materials used in terrorist acts, thereby helping to apprehend the perpetrators.

PARTNERS	COUNTRY
INDRA SISTEMAS S.A. (INDRA)	Spain
AGENZIA NAZIONALE PER LE NUOVE ECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE (ENEA)	Italy
ASTRIUM S.A.S. (ASTRIUM)	France
PANEPISTIMIO THESSALIAS (UNIVERSITY OF THESSALY) (UTH)	Greece
SPACE APPLICATIONS SERVICES NV (SAS)	Belgium
ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (APL)	Poland
NATIONAL BUREAU OF INVESTIGATION (NBI)	Finland
MINISTERIO DELLA DIFESA (RACIS)	Italy
PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW (PIAP)	Poland
SOCIETE NUCLETUDES SA (NUCLETUDES)	France
MINISTERIO DEL INTERIOR (CNP)	Spain
MINISTERE DE L'INTERIEUR (LCPP)	France

HOMER / Homemade explosives (HMEs) and recipes characterisation - Capability

Information

Grant Agreement N°
312883
Total Cost
€4,474,991.50
EU Contribution
€3,436,875.00
Starting Date
01/11/2013
Duration
36 months

Coordinator

POLICE SERVICE OF NORTHERN IRELAND
Una Williamson
Head of EU Programme Office
65 Knock Road
Belfast
BT5 6LE
Contact
Una Williamson
Tel: +44 (0)28 90 90 1155
Mobile: +447734909685
E-mail: una.williamson@psni.pnn.police.uk
Website: www.homer-project.eu

Project objectives

The goal of the HOMER project is to implement a study to mitigate the threat of home made explosives (HMEs) from criminal and terrorist elements.

The objectives of the HOMER project are to:

1. Expand the knowledge of European bodies: map and analyse the sources of information that instruct how to prepare HMEs, the required raw materials and precursors, their technical characteristics and the possibilities of their detection using existing technologies.
2. Mitigate the threat presented by HMEs: expand and enhance knowledge on HMEs to serve security and law enforcement agencies in their quest to prevent the use of HMEs to perpetrate attacks.
3. Work to prevent the use of HMEs: detect and classify HMEs in instances when they are used.
4. Deliver sustainable HME content for use: a knowledge management platform – securely accessible by security and law enforcement agencies – flowing from our study.
5. Draft a standard on HME vocabulary and definitions suitable for Europe.
6. Promote the work of the project.

Description of the work

The HOMER project will implement a comprehensive, European study on HMEs including their identification and detection and the prevention of HME threats. The project will establish basic knowledge hitherto unknown about HMEs and develop a knowledge management platform for use by European police and security services to protect the safety of the EU citizen.

The Project has four main pillars:

Data Collection and Analysis. This work area focuses on the collection and analysis of HME information using a HME literature study and internet empirical study to mine and collect publicly available information on HME recipes to establish answers for the most fundamental questions on HMEs. Data collection will also gather information from industry best practices, expert knowledge within the HOMER consortium and experts across Europe.

Knowledge Management focuses on the sustainability of HME knowledge content relating to manufacturing methods, technical characteristics of HMEs, the required raw materials and their impact, detection and classification. This information will be folded into a knowledge management platform to serve law enforcements agencies, European defence and manufacturers.

Case study experiments and validation will demonstrate the use of the project's research for detecting and classifying the HME data. This pillar will involve the project's main end users for developing case studies to test the platform and the information in laboratory conditions and in the field.

Standardisation, dissemination and exploitation will deliver a standardised HME vocabulary and definitions across precursor manufacturers, security providers and law enforcement agencies. This work will provide a recognised standard of vocabulary to assist agencies in working collaboratively to defeat the HME threat.

Expected results

The HOMER project will deliver three main results:

1. A measured step towards a common HME knowledge management base for Europe's law enforcement, security, defence and manufacturers of fertilisers and chemicals.

2. Better knowledge of the chemicals involved in HMEs, and their components and composition.

3. End user access to HME researched content, strengthening their innovation capacity.

The detection of detonators and chemical compositions for bomb making is crucial for homeland security, environmental clean-up and humanitarian efforts.

PARTNERS	COUNTRY
POLICE SERVICE OF NORTHERN IRELAND	United Kingdom
TAMAR ISRAELI ADVANCED QUARRYING CO LTD.	Israel
THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN	Ireland
BUNDESANSTALT FUER MATERIALFORSCHUNG UND-PRUEFUNG	Germany
BLUGARIA DEFENSE INSTITUTE	Bulgaria
THE QUEEN'S UNIVERSITY OF BELFAST	United Kingdom
CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS	Greece
KENTRO EREVNON NOTIOANATOLIKIS EVROPIS ASTIKI MI KERDOSKOPIKI ETAIREIA	Greece
YARA SA	Belgium
MINISTERIO DEL INTERIOR	Spain

HYPERION / Hyperspectral Imaging IED and Explosives Reconnaissance System

© Hyperion

RESEARCH **COMPLETED**

Information

Grant Agreement N°
284585
Total Cost
€4,825,598.75
EU Contribution
€3,458,969
Starting Date
01/08/2012
Duration
31/10/2015

Coordinator

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Department: Defence & Security, Systems and Technology Unit: Weapon Effects and Security of Explosives
Gullfossgatan 6
SE-164 90 Stockholm, Sweden
Contact
Swedish Defence Research Agency
Tel: +46 8 5550 3000
Fax: +46 8 5550 3949
E-mail: registrator@foi.se
Website:
www.hyperion-fp7.eu

Project objectives

The objective of the HYPERION project was to develop and test a system concept for on-site forensic analysis after an explosion. This included tools and procedures for safer use for the stand-off detection and identification of unexploded IEDs. The on-site data generated by the HYPERION system comprise the type and amount of explosive used in the attack, the point of origin of the detonation and an assessment of the type of IED. A crime scene is mapped using 3D-registration where the positions analyzed in detail on-site are marked on the 3D map. The quality-assured data is electronically documented on-site and sent in a timely manner to police at the post-blast scene. One the post-event scene has been secured, laboratory forensic sampling and analysis can begin. In HYPERION, new and validated sampling protocols were developed. The data from the project's system supplemented the work of bomb disposal specialists by creater safer conditions around a crime scene.

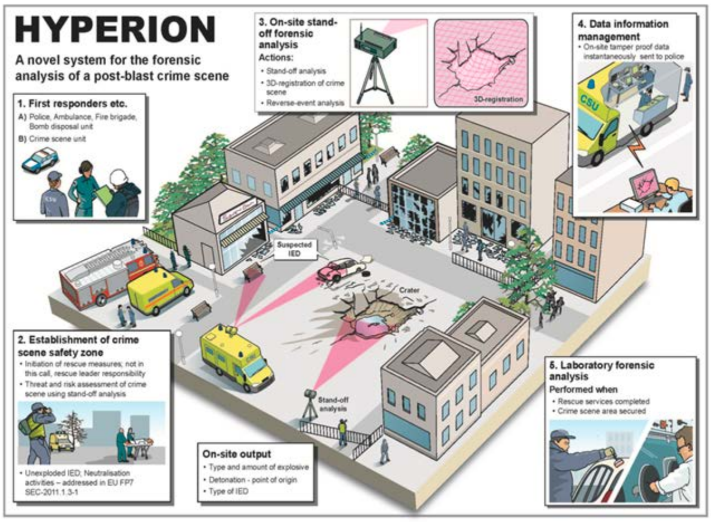
Description of the work

A rapid response from forensic investigations to the police is imperative to increase the chance of finding an attack's perpetrators or to help the police be proactive against attacks such as that of the London Underground (2005) or Madrid train bombings (2004). For police, the first 24 hours is critically importance for a successful crime investigation. This means that a forensic investigation and analysis of a post-blast scene has to be carried out quickly. In addition, it is important that a crime scene's analyis data is of high quality so it can be used as evidence in a trial. Among the kind of information police need to know for investigative purposes is the type and amount of explosive used in an attack. The type of explosive reveals the kind of threat authorities face and may supply hints about where the explosives were obtained. Explosives of the home-made type require the use of a "bomb factory" for their production. The right kind of forensic analysis can provide police with intelligence to localize a bomb factory, which in turn could lead them to the perpetrators of the attack. Also, the point of origin of the detonation is needed to assess the size of the bomb's charge and the type of IED. It is important for the crime investigation to assess if an IED is "VBIED" (Vehicle Borne IED), "PBIED" (Person Borne IED) or "LBIED" (Left Behind IED).

A crime scene area also needs to be well documented using ordinary high-resolution 2D photographs and 3D registration. 3D registration contributes to the calculation of a charge size and point of origin for detonation. Moreover, 3D crime scene registration can be used to register typical damage patterns in the direct vicinity of a crime scene such as damage to buildings. On-site electronic documentation of forensic data is also carried out to preserve the chain of custody.

Results

A system based on HYPERION's concept lead to a reduction in time for delivering forensic evidence requested by police. The faster crime scene investigation is provided, the greater the chances finding the terrorists, thus preventing future attacks. As improved techniques with more sensitive, compact and cost-effective properties emerge and become commercially available, the HYPERION concept can be a future viable tool for police forces.


HYPERION
A novel system for the forensic analysis of a post-blast crime scene
1. First responders etc.
A) Police, Ambulance, Fire brigade, Bomb disposal unit
B) Crime scene unit
3. On-site stand-off forensic analysis
Actions:
• Stand-off analysis
• 3D-registration of crime scene
• Reverse-event analysis
3D-registration
4. Data information management
• On-site tamper proof data instantaneously sent to police
CSU
Suspected IED
Crater
2. Establishment of crime scene safety zone
• Initiation of rescue measures; not in this call, rescue leader responsibility
• Threat and risk assessment of crime scene using stand-off analysis
• Unexploded IED; Neutralisation activities – addressed in EU FP7 SEC-2011.1.3-1
Stand-off analysis
On-site output
• Type and amount of explosive
• Detonation - point of origin
• Type of IED
5. Laboratory forensic analysis
Performed when
• Rescue services completed
• Crime scene area secured

© Hyperion

PARTNERS	COUNTRY
Totalförsvarets forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (FhG-IAF)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
ASELSAN Elektronik Sanayl ve Ticaret A.S. (ASELSAN)	Turkey
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
MORPHO (MPH)	France
VIGO SYSTEM S.A. (VIGO)	Poland
PORTENDO AB (Portendo)	Sweden
ICISLERI BAKANLIGI (EGM)	Turkey
FUNDACION TECNALIA RESEARCH & INNOVATION (TECNALIA)	Spain
RIKSPOLISSTYRELSEN – SWEDISH NATIONAL POLICE BOARD (NFC)	Sweden
SELEX ES SPA (SES)	Italy

LOTUS / Localization of threat substances in urban societies

© paolo toscani - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°
217925
Total Cost
€4,298,595
EU Contribution
€3,189,146
Starting Date
01/01/2009
End date
31/12/2011

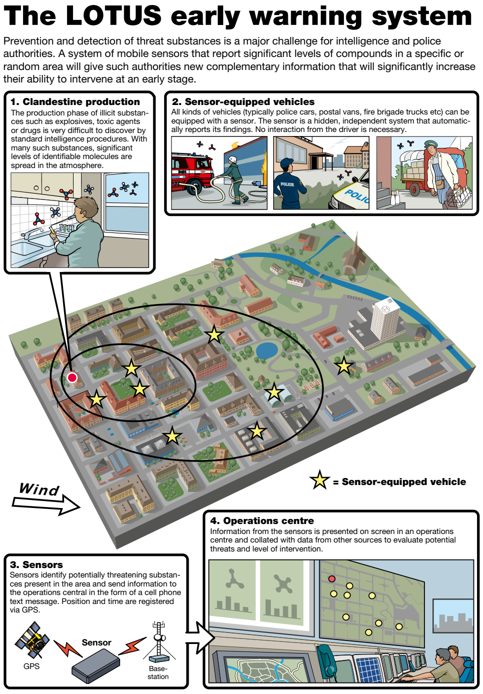
Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Department of Energetic Materials
Grindsjön Research Centre
SE-147 25 Tumba
SWEDEN
Contact
Dr. Sara Wallin
Tel: +46 8 5550 4097
Mobile: +46 709 277008
Fax: +46 8 5550 3949
E-mail: sara.wallin@foi.se
Website: www.lotusfp7.eu

Project objectives

LOTUS set out to develop the software, hardware and concepts of operation needed to deploy an array of mobile and fixed position detection devices to locate explosive precursor chemicals and drugs in urban environments.

The LOTUS team aimed to develop a technical tool for intelligence gathering. This would enable the information obtained to be combined and confirmed with data from other sources (eg. law enforcement investigation) to accurately track and neutralize potential terrorist or organized criminal threats.



The LOTUS early warning system

Prevention and detection of threat substances is a major challenge for intelligence and police authorities. A system of mobile sensors that report significant levels of compounds in a specific or random area will give such authorities new complementary information that will significantly increase their ability to intervene at an early stage.

1. Clandestine production
The production phase of illicit substances such as explosives, toxic agents or drugs is very difficult to discover by standard intelligence procedures. With many such substances, significant levels of identifiable molecules are spread in the atmosphere.

2. Sensor-equipped vehicles
All kinds of vehicles (typically police cars, postal vans, fire brigade trucks etc) can be equipped with a sensor. The sensor is a hidden, independent system that automatically reports its findings. No interaction from the driver is necessary.

3. Sensors
Sensors identify potentially threatening substances present in the area and send information to the operations central in the form of a cell phone text message. Position and time are registered via GPS.

4. Operations centre
Information from the sensors is presented on screen in an operations centre and collated with data from other sources to evaluate potential threats and level of intervention.

© Lotus

Results

A range of sensor mounts was developed and tested by LOTUS for this project. The primary detection method used was air sampling by using sensor units mounted on cars or other mobile platforms that traversed urban spaces.

Ion mobility spectrometers (IMS), differential mobility analysis and IR (infrared) absorption spectroscopy technologies were combined to detect trace elements of explosives or drugs found in the air near bomb-making factories and drug manufacturing laboratories.

Field experiments conducted in Stockholm, Helsinki and Madrid found that trace elements could be positively identified up to 45 metres away, depending on wind, temperature and humidity conditions.

In order to process and report the findings of these sensors, GSM-capable transmitters were built into each unit. These sent data reports, including potential threat detection alerts and GPS coordinates, to a central data fusion hub. Advanced analytical tools were developed to allow the hub to process and categorize readings.

If a potential operational intervention was deemed necessary (i.e. a law enforcement raid), analysis could be carried out with a range of tools to further ascertain the exact location of the threat. To avoid signal interception or pattern detection by potential adversaries, reports from each sensor were heavily encrypted and randomly transmitted.

Another element of the LOTUS system was that no interaction between the vehicle driver and the sensor was required. Indeed, the project proposes that sensors could be mounted on civilian vehicles whose users have no knowledge or need to know about what each sensor is doing.

The result would be a network of sensors randomly surveying urban areas, producing GPS pinpointed reports on potential explosive or drug manufacture locations for central assessment.

PARTNERS	**COUNTRY**
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Portendo AB	Sweden
Saab AB	Sweden
Bruker Daltonik GMBH	Germany
Ramem S.A.	Spain
Bruhn NewTech A/S	Denmark
Research and Education Laboratory in Information Technologies	Greece
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Universidad de Barcelona	Spain
Secrab Security Research	Sweden

OPTIX / Optical technologies for identification of explosives

© Eline Spek - Fotolia.com

Information

Grant Agreement N°
218037
Total Cost
€3,289,855
EU Contribution
€2,487,556
Starting Date
01/11/2008
Duration
54 months

Coordinator

INDRA SISTEMAS S.A.
Security Systems
Paseo del Club Deportivo, 1.
Edif.5
28223-Pozuelo de Alarcón
(Madrid)
Spain
Contact
Carlos de Miguel
Tel: +34 91 257 95 73
Mobile: +34 650 505 091
Fax:+34 91 257 70 18
E-mail: cdemiguel@indra.es
Website: www.fp7-optix.eu

Project objectives

Terrorism, as evidenced by recent tragic events (Madrid 2004, London 2005, New York 2001), is a real and growing threat to Europe and the world. Attacks using Improvised Explosive Devices (IEDs) appear in the news every day. More than 60% of terrorist attacks are carried out by the use of such explosive devices.

Security forces demand new tools to fight against this threat. One of the most demanded capabilities by end users is that of standoff detection and identification of explosives. Today's technologies are not able to provide these capabilities with the required minimum reliability.

The objective of the project is to contribute to increasing the security of European citizens by the development of a transportable system for the standoff detection and identification of explosives in real scenarios at distances of around 20 metres (sensor to target), using alternative or simultaneous analysis by three different complementary optical technologies (LIBS, RAMAN, IR).

Description of the work

The project activities of OPTIX have been broken down into ten work packages and distributed across 42 months.

OPTIX will make important progress beyond the state of the art in three different ways:

» Specific developments regarding the individual core technologies (LIBS, RAMAN and IR) for standoff detection and identification of explosives;

» Specific developments of the enabling technologies being addressed in the project: lasers, spectrometry, optics and data fusion and analysis;

» Integration of all technological developments onto a single system to leverage and enhance the individual capabilities for the standoff detection and identification of explosives.

The first stage will be dedicated to the System Definition. The project consortium will perform focused research on the core optical technologies addressed by the project. Scenarios and system requirements will be defined. This is a key stage for the success and final usefulness of the system from the end user's point of view. Workshops with end users will be organised.

Technology development of LIBS, RAMAN, IR (core technologies) and laser, spectrometry, optics and data fusion (enabling technologies) will follow.

Phase three is System Integration, where a single platform will be developed.

Testing will be carried out in laboratories and also in real environment scenarios, adequately supported by end users. Evaluation of results will follow.

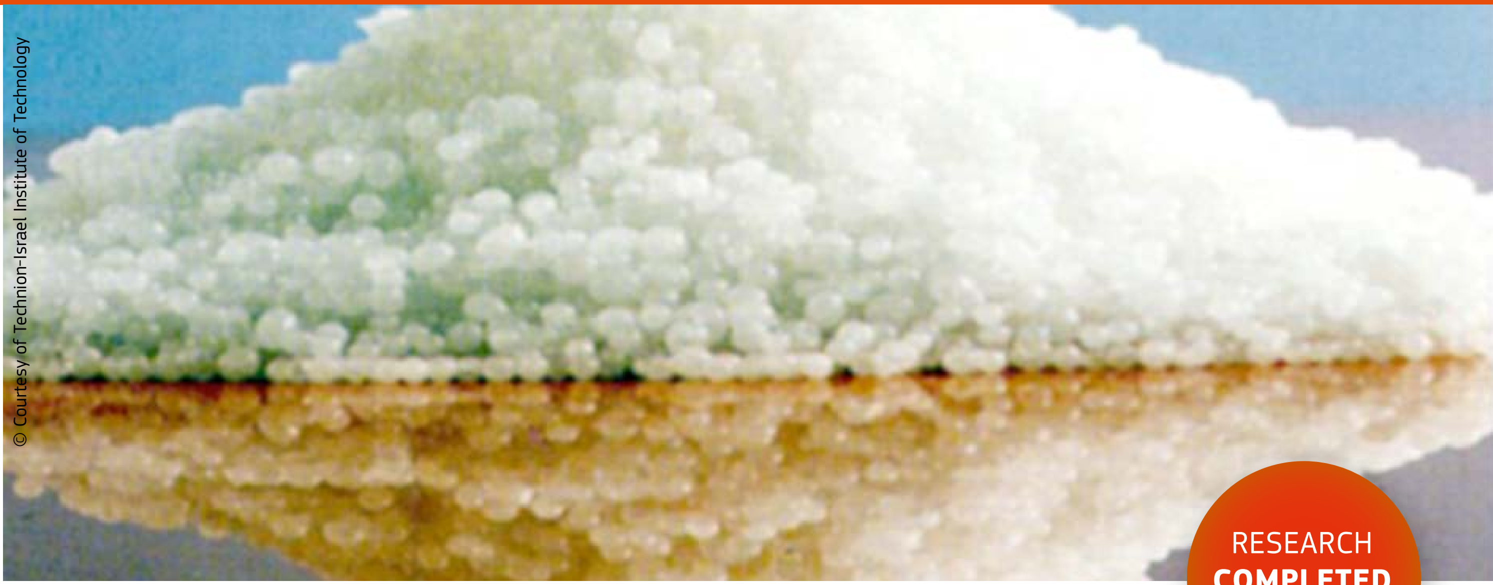
Dissemination and Exploitation will provide information on the project's activities, performance and results both at public and restricted levels, as well as defining and carrying out the initial exploitation of the outcomes and expectations of OPTIX. Workshops with end users and other potential stakeholders will take place.

Expected results

- Improved capabilities of LIBS, RAMAN and IR for the detection of explosives at standoff distances;
- Enhanced spectrometrics for an Integrated OPTIX system;
- Advanced data fusion and chemometrics algorithms;
- A technology demonstrator capable of detecting explosive traces at distances of 20 metres;
- Demonstrated capabilities of the developed system to end users and to additional stakeholders as needed.

PARTNERS	COUNTRY
Indra Sistemas S.A.	Spain
University of Malaga	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
EKSPLA UAB	Lithuania
AVANTES BV.	The Netherlands
Technical University of Clausthal	Germany
Vienna University of Technology	Austria
University of Dortmund	Germany
Guardia Civil	Spain

PREVAIL / PRecursors of ExplosiVes: Additives to Inhibit their use including Liquids



© Courtesy of Technion-Israel Institute of Technology

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241858
Total Cost
€4,296,266.87
EU Contribution
€3,343,162
Starting Date
01/09/2010
End Date
31/10/2013

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Department of Energetic Materials
Gullfossgatan 6
164 90 Stockholm
Sweden
Contact
Malin Kölhed
Tel.: +46 (0)8 5550 4197
Mobile: +46 (0)70 9277010
E-mail: Malin.kolhed@foi.se
Website: www.prevail-fp7.eu

Project objectives

The goal was to prevent or at least make it much more difficult to manufacture explosives. Another part of the project focused on finding a suitable marker/detection system to facilitate detection of illegal use of fertiliser-based homemade explosives, a task that today is very difficult to perform. These objectives had to be met without obstruction of the legitimate use of these products and without causing any adverse effects on the environment or on people's health.

Description of the work

The PREVAIL project focuses on finding inhibitors to add to some precursors to prevent them from being used to produce home made explosives or to prevent them from being concentrated by boiling water. A second goal in the PREVAIL project is to find markers to add to certain precursors to ensure easier detection. PREVAIL will perform research into a marker/detection system rather than just the markers, in order to ensure detectability of the markers. The markers found must be environmentally friendly, non-toxic and bio-degradable. Honey bees, micro crystals and fluorescence light will be tested as detectors for these added markers, and micro encapsulation will be used for slow and controlled release. For a successful project, the objectives must be met: without causing any adverse effects on the environment or on people's health and without obstructing the legitimate use of these materials. Since this project will strongly influence manufacturers, users, legislators and governmental security agencies, the ties between the project and the stakeholders are strong. The industrial partners will identify if added inhibitors and markers need extra testing for safety. A road map for future Research and Development work and actions (as well as regulatory) will be prepared.

Results

Results regarding selected project objectives:

» Inhibitors to prevent the concentration of a precursor

The final candidate was tested for inhibition activity, stability and removal in lab scale and was finally validated in large scale and long-term testing. This showed that it is possible to find chemicals that function in the desired temperature range. The inhibition activity of these chemicals will make it much more difficult to construct bombs using the precursor under study. However, the stability should be further improved. Future research methods have been identified.

» Inhibitors for preventing the formation of some home-made explosives crystals

These inhibitors were tested for activity and removal on lab scale and were finally validated on a realistic scale and the results are promising.

If this measure is implemented, we all shall benefit from the fact that terrorists will encounter major difficulties when attempting to prepare this HME.

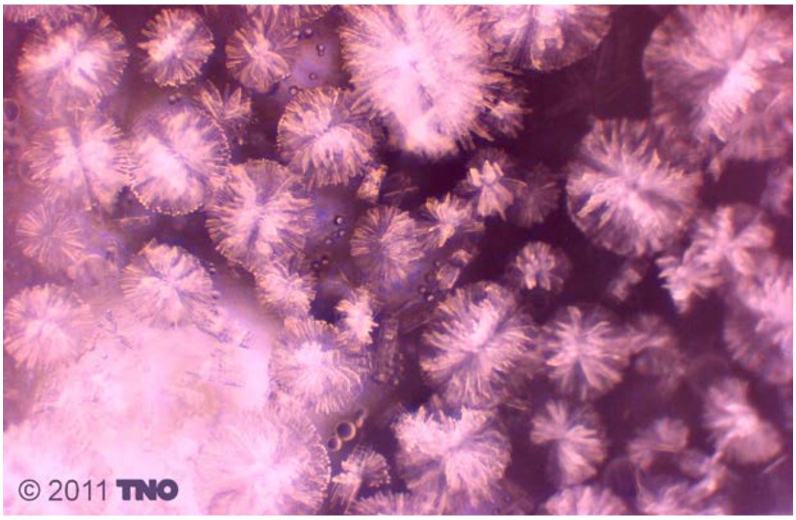
» Novel Markers for fertiliser-based homemade explosives

These markers were developed to suit specific detectors, as well as to be environmentally friendly, non-toxic and bio degradable.

The work has found technical solutions of where to add a chemical marker in order to be able to detect illegal uses of fertilisers. The work has also resulted in a unified work with the European coatings industry. Further research will be necessary to find technological detection solutions that can be implemented.

» Roadmap for future work

A roadmap for future Research and Development work and actions (as well as regulatory) was prepared. Criteria for the industrial implementation of inhibitors and markers were drafted. The usefulness of the developed additives for other precursors was also assessed and required future research was indicated.

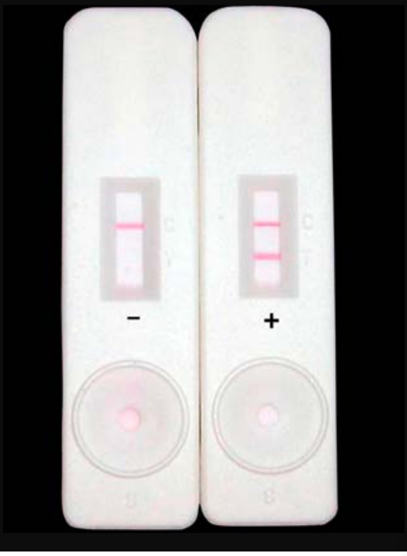

© 2011 TNO

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Technion – Israel Institute of Technology (Technion)	Israel
Arkema France (Arkema)	France
KCEM AB (KCEM)	Sweden
Yara International ASA (Yara)	Norway
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Wojskowy Instytut Higieny i Epidemiologii (WIHiE)	Poland
SECRAB Security Research (SECRAB)	Sweden
Inscentinel Ltd. (INSC)	United Kingdom

SALIANT / Selective Antibodies Limited Immuno Assay

Novel Technology

© SALIANT



RESEARCH **COMPLETED**

Information

Grant Agreement N°
242377
Total Cost
€4,498,088.80
EU Contribution
€3,362,598.60
Starting Date
01/09/2010
End Date
31/12/2013

Coordinator

UNIVERSITY OF NEWCASTLE UPON TYNE
Institute of Cellular medicine
Kensington Terrace 6
NE1 7RU, Newcastle Upon Tyne
United Kingdom
Contact
Colin Self
Tel.: +44 191 223 5604
Fax: +44 191 223 5601
E-mail: c.h.self@ncl.ac.uk
Website: http://www.saliant.eu/

Project objectives

SALIANT is focussed on developing a hand-held device for real-time analysis of trace levels of explosives, chemicals and drugs. The key innovation is a positive detection lateral-flow test for small molecules that is highly sensitive and simple to use making it ideally suited to deployment by First Responders at crime scenes and terrorist incidents.

SALIANT offers a system based on a small bindable moiety that is first conjugated close to the binding site of a primary antibody against the analyte such that when analyte binds the antibody, the moiety can still be bound by a labelled secondary antibody. A large reagent-analogue of the analyte is also introduced, binding the analyte-unbound primary antibody, and thereby blocking binding of the secondary antibody to the moiety. Thus the more analyte present, the more binding of secondary antibody occurs and more signal is produced.

Description of the work

Lateral flow immunodiagnostics has long offered the promise of fast, high-quality testing for substances of low molecular weight. There have however been very real challenges to bringing the full power of such technology to bear in this area. What is required is a robust system in which there is no observable signal in the absence of analyte, and even low-level samples give an obvious observable signal over this zero background.

The SALIANT project is divided into several technical work packages which comprise research and development of sampling and detection methods, technology integration and demonstration of practical device application in forensic laboratories and first responder scenarios.

An initial specification process will ensure that target molecules and application scenarios are catered for in the development of sampling technologies. This is followed by development of the SAL Universal detection system and in parallel the development of the Apposition detection system to give complementary dipstick and read-out systems respectively. The device will be further developed and integrated with sampling and detection technologies before practical demonstrations in both laboratory and first responder scenarios.

A work package is also dedicated to the dissemination of results which will not only spread awareness of the knowledge gained between project partners and the wider security industry research and technology community but also promote and develop synergy between the security sector, security industry and academia through common training activities and workshops.

Results

SALIANT has been highly successful in meeting its objectives of designing and developing an ultra-rapid testing platform for the high explosives RDX, PETN, HMX and TNT that is very simple to deploy and complementary to physical methods of detection. A key feature of the system is that the presence of explosive is positively seen on a dipstick simply as a positive red line, over a white zero background, that is easy to see by eye or read with a hand-held reader. The lateral flow dipstick systems that have been developed are capable of simple visual detection within seconds of sample application and quantitative detection within a few minutes. This capability has been complemented by development of highly efficient sampling means, including rapid surface-wipe and air sampling devices and protocols. The programme has also facilitated development of a hand-held reader allowing rapid quantification, storage and controlled broadcasting of results. Extensive laboratory and field-testing, following controlled explosions, have clearly shown the robustness and excellent performance of the systems. The high sensitivity (to parts per billion) speed and simplicity of use of the devices allows their application to both post-blast incidents and pre-blast screening applications by personnel such as first responders and security staff. The SALIANT consortium has developed the complete high performance detection package to a fully developed pre-manufacturing production prototypic stage.

PARTNERS	COUNTRY
University of Newcastle upon Tyne (UNEW)	United Kingdom
Selective Antibodies Limited (SAL)	United Kingdom
OY REAGENA Ltd (REAG)	Finland
Indicia Biotechnology (IND)	France
Department of Justice, Equality & Law reform (FSL)	Ireland
Zilinska univerzita v ziline (UNIZA)	Slovakia
Netherlands Forensic Institute (NFI)	The Netherlands
Applikon Analyzers (APP)	The Netherlands
Stichting Dienst Landbouwkundig Onderzoek (DLO-FBR)	The Netherlands
Centre of Excellence for Life Sciences Ltd (CELS)	United Kingdom
Kite Innovation (Europe) Limited (KITE)	United Kingdom

SUBCOP / Suicide Bomber Counteraction and Prevention

© freeimages – Andreas Krappweis

Information

Grant Agreement N°
312375
Total Cost
€4,601,647.25
EU Contribution
€3,486,040.00
Starting Date
01/06/2013
Duration
36 months

Coordinator

SWEDISH DEFENCE RESEARCH AGENCY (FOI)
Department of Weapon Effects and Security of Explosives
Gullfossgatan 6
SE-164 90 Stockholm,
Sweden
Contact
Anna Pettersson
Tel.: +46 8 5550 4027
Mobile: +46 709 277224
Fax: +46 8 5550 3949
E-mail:
anna.pettersson@foi.se
Website: www.subcop.eu

Project objectives

SUBCOP addresses the extraordinary challenge of how to intervene in a suicide bombing event using non-lethal means.

SUBCOP sets out to develop technologies and procedures that can be applied by police security forces when responding to a suspectedperson-borne improvised explosive device)(PBIED). The core objectives for SUBCOP are to consider the:

» available technological tools for less than lethal PBIED intervention,

» novel procedures for their application, and

» development of new technological capabilities.

SUBCOP addresses the course of action to take when an alert to a possible PBIED has been issued and an attack may be imminent. The project recognises that an alert may only give cause for suspecting the presence of a PBIED, and that this suspicion can be of lower or higher confidence. SUBCOP will develop guidance for responses to a PBIED that are ethically and socially justifiable, given the context.. SUBCOP is insensitive to how the alert is raised, whether based on detection of explosives or explosive devices, informants' reporting or other intelligence sources.

Description of the work

The selection of tools and technologies for countering a PBIED event requires an understanding of the operational and situational requirements for end-user intervention. In the first phase of the project, requirements are collected from end users that either have or would be responding to a PBIED event. In parallell, previous PBIED events are analysed in detail in order to gain a deeper understanding about the underlying factors in PBIED attacks. The selection of tools and technnologies are further supported by a technical capability and gap analysis.

The project focuses its technical work on three different areas:

» Supporting and softer methods encompasses situational awareness tools, psychological approaches and methods to direct the crowd away from the danger;

» Mitigation and containment brings rapidly deployable physical protection from the effects of the IED in case of an explosion. It also surveys possible electronic warfare measures that can be used in an urban environment to mitigate remote initiation of the IED;

» Less than lethal methods focuses on existing and emerging tools and technologies for engaging with the suspect to achieve immediate but reversible incapacitation. Evaluation of promising tools and new developments are part of the project objectives in this area.

The selection of tools to be further investigated and developed within SUBCOP is based not only on the efficiency of the countermeasures to handle the PBIED, but also on the medical risks and risks of collateral injuries to the suspect, law enforcement personnel or bystanders caused by countermeasures. It must be understood that the outcome of a PBIED situation can be highly lethal.

The potential responses to PBIED situations can be assessed by end users in a preparatory phase through the toolbox model, which incorporates the tools' efficiency, utility and safety when applied in a PBIED context.

The project embeds ethical aspects into the tools' selection and their modelling. Ethical and legal aspects of research and deployment are also part of the project work plan.

Expected results

SUBCOP will develop technology demonstrators and suggest tools and procedures for use in PBIED situations. A response guidance training tool for assessing response strategies applied in the separate-, protect- and engage-phases of PBIED intervention is another major output of the project.

In the final phases, the outcome of SUBCOP will be a training-and-validation exercise for end users.

In the long term, the project will help prepare police forces throughout the EU in dealing with PBIED terrorist attacks.

PARTNERS	COUNTRY
Swedish Defence Research Agency (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
ASELSAN Elektronik Sanayi ve Ticaret A.s. (ASELSAN)	Turkey
RAND Europe Community Interest Company (RAND)	United Kingdom
Franhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V. (FhG-ICT)	Germany
CBRNE Ltd. (CBRNE)	United Kingdom
Cerberus Black Ltd. (CB)	United Kingdom
Karolinska institutet (KI)	Sweden
Icisleri Bakanligi (EGM)	Turkey
Technische Universiteit Eindhoven (TU/e)	The Netherlands
Ministry of Public Security (MOPS-INP)	Israel

TIRAMISU / Toolbox Implementation for Removal of Anti-Personnel Mines, Submunitions and UXO

© TIRAMISU

Information

Grant Agreement N°
284747
Total Cost
€19,798,269.08
EU Contribution
€14,934,745
Starting Date
01/01/2012
Duration
48 months

Coordinator

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
Polytechnic Faculty
30, Avenue de la Renaissance
1000 – Brussels - Belgium
Contact
Yvan Baudoin
Tel: +32 2 7426553
Fax: +32 2 7426547
E-mail:
yvan.baudoin@rma.ac.be
Website: www.rma.ac.be

Project objectives

Anti-personnel landmines and unexploded ordnance (UXOs) represent an important obstacle in the transition from crisis to peace for war-affected countries. They threaten post-conflict development and welfare.

The objective of the TIRAMISU project is to provide the Mine Action community with a toolbox to assist in addressing the many issues related to Humanitarian Demining and thus promoting peace, national and regional security, conflict prevention, social and economic rehabilitation and post-conflict reconstruction.

The tools in development are divided in two main categories:

» Demining planning tools, which will help locate the threats and define the contaminated areas;

» Detection and disposal tools, which will physically neutralise mines and UXOs and improve operators' safety. In this context, in-depth training will be provided to the users.

These tools will be tested and validated in mine-affected countries and will also benefit from state-of-the-art technologies (robots, UAV...).

Description of the work

TIRAMISU is divided into 10 modules that will cover all the different aspects of Humanitarian Demining. They are:

» Land Impact Survey: tools enabling the prioritisation of the areas most affected and the efficient use of the other modules in a given situation. These tools will make use of remote sensing and decision support systems;

» Non-Technical Survey & Advanced General Survey: tools to facilitate land release;

» Technical Survey: tools to detect indicators of probable presence of landmines/UXOs;

» Ground-based Close-in Detection: tools, such as advanced metal detectors, Ground Penetrating Radars and novel chemical sensors;

» Stand-off Detection: tools to detect mines, submunitions or explosives at close range with remotely controlled Micro (Unmanned) Aerial Vehicles (MAV/UAV) or flying biosensors (honeybees);

» Disposal of ERW (Explosive Remnants of War): tools to protect deminers or vehicles against explosions;

» Mine Risk Education: tools to assist in Mine Risk Education activities;

» Training: tools aiming at developing capacity building and enabling the user uptake of the tools developed;

» Mine Action mission management: tools to improve planning and execution of Mine Action missions;

» Standards: this module includes the current and in-progress or proposed CEN Workshop Agreements (CWA).

In order to test the tools and to also increase the confidence of the Mine Action community in these tools, test and validation campaigns will be organised in several mine-contaminated countries.

The project is steered by two boards that will be involved in every step of the development of TIRAMISU to ensure that the tools being developed will really be useful to the Mine Action community. The End-User Board will assist in the definition of the needs and the assessment of the usefulness of the tools. The Project Advisory Board will provide an independent view on the tools' design and development and on any ethical issues that could arise in the course of the project.

Expected results

The TIRAMISU Toolbox will offer a comprehensive modular structure covering the different Mine Action processes, from Land Impact Survey to the safe Mine Clearance Actions and disposal. The tools will be designed with the active participation of end-users, and tested and validated in mine-contaminated countries.

It is expected that these tools will benefit Mine Action Centres and national Mine Action authorities, private companies and NGOs working in Mine Action, as well as European and UN agencies.

PARTNERS	COUNTRY
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
UNIVERSITA DEGLI STUDI DI GENOVA (DIMEC)	Italy
DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV (DLR)	Germany
INSTITUTO DE SISTEMAS E ROBOTICA-ASSOCIACAO (ISR-UC)	Portugal
AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES (CSIC)	Spain
UNIVERSITA DEGLI STUDI DI CATANIA (UNICT)	Italy
INSTYTUT MASZYN MATEMATYCZNYCH (IMM)	Poland
DIALOGIS UG (HAFTUNGSBESCHRANKT) (DIALOGIS)	Germany
SVEUCILISTE U ZAGREBU - GEODETSKI FAKULTET (FGUNIZ)	Croatia
HRVATSKI CENTAR ZA RAZMINIRANJE-CENTAR ZA TESTIRANJE RAZVOJ I OBUKU DOO (CTDT)	Croatia
NOVELTIS SA (NOVELTIS)	France
PARIS-LODRON-UNIVERSITÄT SALZBURG (PLUS)	Austria
WOJSKOWY INSTYTUT TECHNIKI INZYNIERYJNEJ IM PROFESORA JOZEFA KOSACKIEGO (WITI)	Poland
THE UNIVERSITY COURT OF THE UNIVERSITY OF ST ANDREWS (USTAN)	United Kingdom
UNIVERSITE LIBRE DE BRUXELLES (IGEAT)	Belgium
SPINATOR AB (SPINATOR)	Sweden
PROTIME GMBH GESELLSCHAFT FUR INFORMATIONSLOGISTIK (PROTIME)	Germany
SPACETEC PARTNERS SPRL (STP)	Belgium
EUROPEAN UNION SATELLITE CENTRE (EUSC)	Spain
VALLON GMBH (VALLON)	Germany
I.D.S. - INGEGNERIA DEI SISTEMI - S.P.A. (IDS)	Italy
PIERRE TRATTORI DI GIOVANNI BATTISTA POLENTES & C SNC (PIERRE)	Italy
BRIMATECH SERVICES GMBH (BRIMATECH)	Austria
COMITE EUROPEEN DE NORMALISATION (CEN)	Belgium

IMSK / Integrated mobile security kit

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218038
Total Cost
€23,485,135.25
EU Contribution
€14,864,308
Starting Date
01/03/2009
End Date
28/02/2013

Coordinator

SAAB AB
Saab Microwave Systems
SE-412 89 Göteborg
Sweden
Contact
Daniel Forsberg
Tel: +46 31 794 9123
Fax: +46 31 794 9475
E-mail: daniel.forsberg@saabgroup.com

Project objectives

The Integrated Mobile Security Kit (IMSK) project aims at increasing the security of citizens in the scope of events gathering a large number of people, such as medium to large scale sports events (from football games to the Olympic Games), political summits (G8 summit) etc. The security related to these types of events with intense mass media coverage has indeed become an increasing concern due to new threats of terrorism and criminal activities (such as suicide bombers, improvised explosive devices, increasingly credible CBRN threats).

To counter this situation, new systems are needed that can cover various security aspects and allow for cooperation between different stakeholders. The systems need to be mobile and adaptable in order to address situations of different kinds and different locations. The main objective of the proposed project is the study, development, assessment and promotion of such a system, the IMSK, providing emerging solutions for increased probability of rapid detection and response to threats.

Description of the work

The Integrated Mobile Security Kit (IMSK) project will combine technologies for area surveillance, checkpoint control, also CBRNE detection and support for VIP protection, into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc.) which temporarily need enhanced security. The IMSK accepts input from a wide range of sensor modules, either legacy systems or new devices brought in for a specific occasion. Sensor data will be integrated through a (secure) communication module and a data management module and output to a command & control centre.

IMSK will have an advanced man-machine interface using intuitive symbols and a simulation platform for training. End-users will define the overall system requirements, ensuring compatibility with pre-existing security systems and procedures. IMSK will be compatible with new sensors for threat detection and validation, including cameras (visual & infra-red), radar, acoustic and vibration, x-ray and gamma radiation and CBRNE.

Tracking of goods, vehicles and individuals will enhance situational awareness, and personal integrity will be maintained by the use of, for example non-intrusive terahertz sensors. To ensure the use of appropriate technologies, police and counter-terrorist operatives from several EU nations have been involved in defining the project in relevant areas.

Close cooperation with end-users will ensure compatibility with national requirements and appropriate interfaces with existing procedures. The effectiveness of IMSK will be verified through field trials. Through IMSK, security of the citizen will be enhanced even in asymmetric situations.

Results

IMSK designed a system to optimally integrate different sensor information feeds to produce a common operational picture for area surveillance checkpoint control and detection of CBRNE (chemical, biological, radiological, nuclear, explosive) threats during large-scale events. The goal was also to provide security support to protect important public figures and others who might be present during such event.

Sensor data was integrated via a secure communication module and a data management module and output to a command & control centre. The technologies' sensor data was fed into a single information platform and fused to create a common picture for rapid distribution at event sites (hotels, sport or festival arenas, etc.) which temporarily need enhanced security.

IMSK developed an information model – the "Mobile Situation Object" –used for information-gathering from all its subsystems and their sensors.

The project's heart is its command and control subsystem (C2), which allows authorities to monitor a site and activity by humans, vehicles and other factors. The "position" of a threat could be continuously updated as well as that of security forces.

IMSK also developed sensors for CBRNE detection, 3D face recognition and the detection of hidden weapons via passive THz technology. It studied security procedures currently used across Europe in order to better frame future European standard operating procedures.

The IMSK team says its technology could increase the volume of visitors moving through security checks, while allowing for a reduction in the number of security personnel required.

PARTNERS	**COUNTRY**
Saab AB	Sweden
Selex Sensors and Airborne Systems Limited	United Kingdom
Selex Communications S.p.A.	Italy
Telespazio S.p.A.	Italy
Cilas	France
Diehl BGT Defence GmbH & CO KG	Germany
Thales Security Systems SA	France
Bruker Daltonik GmbH	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Ministère de l'intérieur- STSI	France
Universita Degli Studi Di Catania	Italy
Thyia Tehnologije d.o.o.	Slovenia
AS Regio	Estonia
EPPRA S.A.S	France
Qascom S.r.l	Italy
Rikskriminalpolisen - Swedish National Police Board	Sweden
Regione Lombardia	Italy
Thales Research and Technology Ltd	United Kingdom
TriVision ApS	Denmark
Joint Research Centre (JRC)	Belgium
Deutscher Fußball-Bund e.V.	Germany
AirshipVision International S.A	France
University of Reading	United Kingdom
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom

RAPTOR / Rapidly deployable, gas generator assisted. inflatable mobile security kits for ballistic protection of European civilians against crime and terrorist attacks

© BAYRAM TUNÇ - istockphoto.com

Information

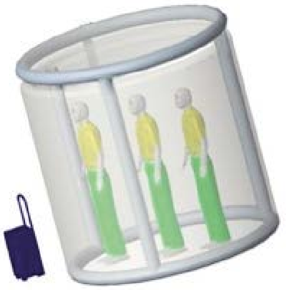
Grant Agreement N°
218259
Total Cost
€2,849,867.76
EU Contribution
€2,060,995.13
Starting Date
01/01/2010
Duration
48 months

Coordinator

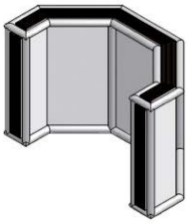
FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institut für Chemische Technologie (ICT)
Joseph-von-Fraunhofer-Str. 7
76327 Pfinztal (Berghausen),
Germany
Contact
Dr. Norbert Eisenreich
Tel +49 721 4640 138
Fax +49 721 4640 538
E-mail: norbert.eisenreich@ict.fraunhofer.de
Website:
http://www.raptor-project.eu/
http://www.ict.fraunhofer.de/

Project objectives

The aim of the RAPTOR project is the development of a mobile, rapidly deployable and inflatable structure for ballistic protection. The project consortium is working on specific solutions to support European security forces in the prevention of, or response to, various threat scenarios. Emphasis is placed on the protection of individuals, general security at events and the protection of humanitarian workers, such as Red Cross employees.


© Raptor

Isometric View without covering



Description of the work

- Definition of threat scenarios such as acts of terrorism and organised crime. Based on these scenarios, specifications for the development of the security kit are defined and criteria for the demonstration of their effective performance derived;
- Development of textiles and coatings for ballistic protection with respect to foldability, light weight and environmental influence;
- Development of textiles and coatings for inflatable structures and suitable coverings for transport and storage;
- Development and characterization of a gas generator formulation with high mass specific gas output, low gas temperature and non-toxic gas components;
- Evaluation and testing of combustion chamber designs with respect to small size and light weight;
- Consolidation of the demonstrators will comprise the incorporation of all basic systems, e.g. gas generator, ballistic protection design and the inflatable structure;
- The final tests of the demonstrators will be done according to the defined threat scenarios. The results will be reviewed according to the goals set out at the start of the project;
- Development of a dissemination plan of the results and knowledge obtained in the project;
- Overall Project Management and Co-ordination, Accounting, Quality Assurance & Control.

Expected results

- Compilation of threat scenarios;
- Performance requirements of protection kit;
- Selection of ballistic protection textiles appropriate to security kit requirements;
- Development of textiles and coatings for inflatable structures;
- Ballistic testing to explore the effectiveness of multi-layer set-up;
- Gas generator composition characterised by high gas output and fast burning behaviour;
- Consolidation and final testing of demonstrators;
- Innovation plan, exploitation plan and feasibility study.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT)	Germany
Bundeskriminalamt (BKA)	Germany
Dr. Lange GmbH & Co KG (LANCO)	Germany
Explosia a.s. (EXPLOSIA)	Czech Republic
P-D Interglas Ltd. (INTERGLAS)	United Kingdom

TACTICS / Tactical Approach to Counter Terrorists in Cities

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285533
Total Cost
€4,466,999.07
EU Contribution
€3,478,464.00
Starting Date
01/09/2012
End Date
31/08/2015

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK TNO
Human Behaviour and Organisational Innovations
Brassersplein 2
Postbus 5050, 2600 GB, Delft
2612CT, Delft,
The Netherlands
Contact
Sharon Prins
Tel +31 88 86 67766
Mobile: +31 6 53715812
E-mail: sharon.prins@tno.nl, info@fp7-tactics.eu
Website: www.tno.nl, www.fp7-tactics.eu

Project objectives

The objectives of TACTICS were to identify, research and develop tools, technologies and methods to improve the effectiveness of security forces in preventing and dealing with an urban attack or threat, while taking fully into account legal requirements, democratic and ethical principles.

The Scientific and Technical goals of TACTICS were:

1. Improving the threat decomposition process
2. Improving the capability management process
3. Supporting the threat management process
4. Developing a three-levelled facilitation approach
5. Implementing legal requirements, democratic and ethical principles into the research and development process within TACTICS

TACTICS supported each of these managers in reacting more quickly and in a more structured, efficient way to a specific threat by delivering a powerful TACTICS Decision Support System that supported the responding to threats and minimized the consequences of a terrorist attack in an urban environment.

Description of the work

The work started by gaining a common view on the TACTICS problem definition and the desired solution.

Possible attack scenarios were sketched and two were chosen together with the end users that were consulted during a workshop in December 2012. The TACTICS concept of operations was also simulated with this group.

Building on this work, the TACTICS system architecture was designed in more detail based on a vision for a TACTICS-type-of-system, and the system architecture of our concrete validation system. This included specifying what privacy-by-design, user centered design means for these kinds of systems, and for the concrete validation system. For a limited set of emerging surveillance methods and technologies their potential contribution to the TACTICS concept was described.

A large number of historical attacks were analyzed in a structured non-biased way. The (non) functional requirements for the three TACTICS components TM, TDM and CM were designed and documented, after which they were built. The data fusion engine was defined and a non-biased method for both threat analysis and capability analysis has been developed. The TM, TDM and CM were evaluated by the end users in a validation workshop in September 2014.

Throughout the project ethical aspects are taken into account and this is reflected in an ethical paragraph in the majority of the deliverables.

Results

TACTICS aimed to increase the effectiveness and efficiency of end users and stakeholders:

End user focus:
TACTICS increased effectiveness and efficiency of the following end user responsibilities in the case of the prevention of a specific threat or dealing with an actual attack:

» Police officers: patrolling the streets and other public places, maintaining public order, providing assistance in emergencies.

- Military Police: maintaining public order, providing assistance in ceremonial duties, personal protection.
- Private security: personal protection, protection of small companies (e.g. shops), protection of bigger closed urban environments (e.g. malls, concert halls or universities).

TACTICS increased effectiveness and efficiency of the following *stakeholder responsibilities* that were relevant for the prevention of a specific threat or dealing with an actual attack:

- National coordinators for counterterrorism: analysing intelligence and other information, policy development, coordinating anti-terrorist security measures.
- Local municipalities: managing safety and security in their own town or city.
- National security services: investigating individuals and organizations, promoting the security of vital sectors, gathering international intelligence and compiling risk and threat analyses.
- Pan-European authorities: promoting information sharing to address free movement of persons and ensure European-wide public safety.their own town or city.

PARTNERS	COUNTRY
Nederlandse Organisatie voor toegepast natuur-wetenschappelijk onderzoek (TNO)	The Netherlands
Rand Europe (RAND)	United Kingdom
Korps Landelijke Politiediensten (KLPD)	The Netherlands
Peace Research Institute Oslo (PRIO)	Norway
ITTI Sp. Z o.o. (ITTI)	Poland
LERO @ TRINITY COLLEGE DUBLIN (TCD)	Ireland
International Security and Counterterrorism Academy (ISCA)	Israel
Universidad Politécnica de Valencia (UPV)	Spain
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (FHG)	Germany
Koninklijke Marechaussee (KMAR)	The Netherlands
Morpho (MPH)	France

UNCOSS / Underwater coastal sea surveyor

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218148
Total Cost
€4,119,638.72
EU Contribution
€2,763,818.61
Starting Date
01/12/2008
End Date
31/07/2012

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Le Ponant de Paris
25 Rue Leblanc
F-75015 Paris Cedex 15
France
Contact
Guillaume Sannie
Tel: +33 1 69 08 51 88
Website:
http://www.uncoss-project.org/

Project objectives

The waterways are becoming more and more crucial for coastal economy and paradoxically, such areas remain very vulnerable to terrorism attacks especially against underwater IED threats. Coastal regions such as in southern Europe and south-east Asia are contaminated by different ammunition left on the sea bottom after war activities from World War I, II and more recent conflicts. This represents a constant threat to the sea traffic, fishermen, tourists and local populations. The objects on the sea bottom are of different natures and include torpedoes, airplane bombs, anti-ship mines, grenades, gun fuses, ammunition and projectiles of different calibers. For example, it is estimated that there are at least 130 000 tons of explosive devices in the eastern coastal waters of the Adriatic Sea. This dramatic pollution weakens the economic development capacity of such regions.

A major challenge is to provide new tools for keeping naval infrastructure safe: harbours, ships, coastal areas, ferry terminals, oil and gas terminals, power/nuclear plants, etc. The main objective of the UNCOSS project is to provide tools for the non-destructive inspection of underwater objects mainly based on neutron sensors. The technology used has already been experimented with for Land Protection (especially in the frame of the FP6/Euritrack project). The application of this technology for underwater protection will be a major achievement.

The classic approach to underwater IED detection is mainly based on sonar detection (derived from military development for mine clearance) which can not guarantee if unattended objects contain explosive. The identification/classification of underwater objects using classical sensors such as sonar and video cameras, becomes more and more difficult when facing asymmetrical attacks. The UNCOSS project is a cost-effective response to new terrorism threats and provides a fundamental technology for the global issue of maritime surveillance and port/naval infrastructure protection.

There is no specific device capable of identifying explosive contents of submerged UneXplode Ordnance (UXO) therefore Explosive Ordnance Disposal (EOD) teams at present have to remove the objects without knowledge of the explosive charge presence.

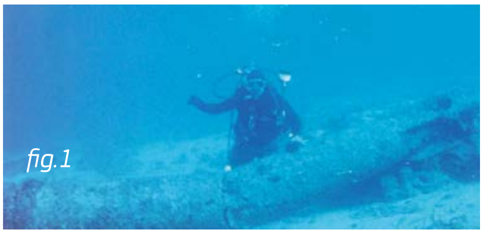


fig.1

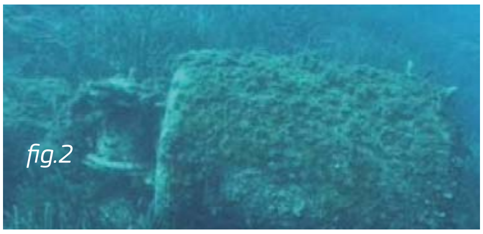


fig.2

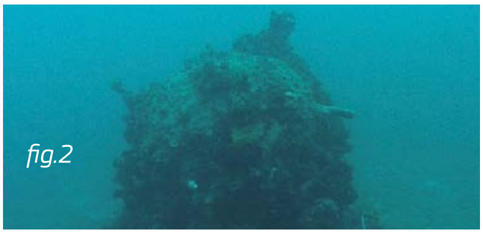


fig.2

© Uncoss

Figure 1: Torpedo from World War II
Figure 2: Antiship mines

Results

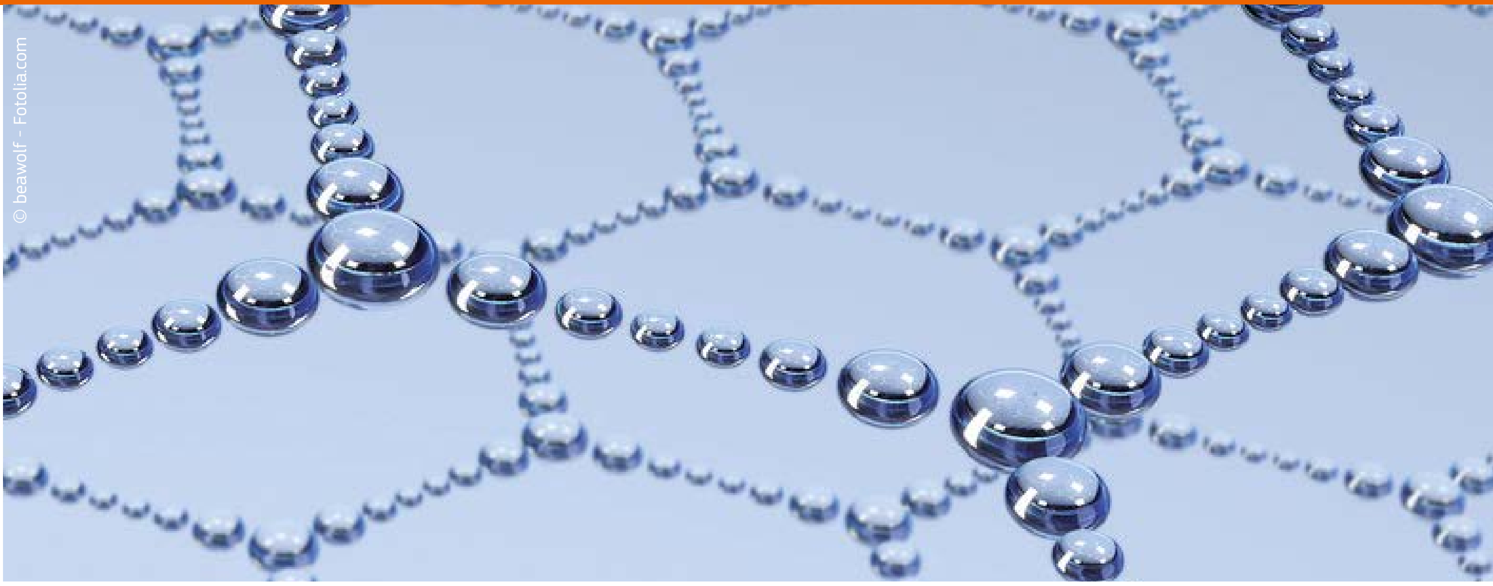
The project's main objective was to provide tools for the non-destructive inspection of underwater objects based on a neutron generator and gamma sensor. The technology's application for underwater protection is one of its major achievements.

UNCOSS designed, manufactured and tested a remotely operated vehicle (ROV) to inspect suspicious objects lying on the seafloor or riverbed. The ROV hovers over an object and reads its chemical make-up using the neutron generator and gamma sensors. The range of the reading depends on the salt content of the water and varies from several centimetres in very salty water to several meters in freshwater.

The project's underwater neutron inspection system was tested in Croatia's Punat Seaport to prove its ability to distinguish explosive surrogates from sediments in metallic objects lying on the seafloor. A further demonstration was performed along's Slovenia's Adriatic seacoast, which demonstrated that the ROV can detect metallic objects potentially buried in the seabed.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
ECA S.A.	France
Ruder Boskovic Institute (RBI)	Croatia
Laseroptronix	Sweden
Jozef Stefan Institute (JSI)	Slovenia
A.C.T.d.o.o. (ACT)	Croatia
Port Authority Dubrovnik	Croatia
Port Authority Bar	Montenegro
Port Authority Vukovar	Croatia
Mednarodna podiplomska šola Jožefa Stefana (MPS)	Slovenia

VIRTUOSO / Versatile information toolkit for end-users oriented open sources exploitation



© beawolf - Fotolia.com

Information

Grant Agreement N°
242352
Total Cost
€11,497,567.53
EU Contribution
€7,999,182.55
Starting Date
01/05/2010
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Centre de Saclay- Bât 476
F91191 Gif-Sur-Yvette
Cedex
France
Contact
Géraud Canet
Tel: +33 1 46 54 82 59
Fax: +33 1 46 54 75 80
E-mail: geraud.canet@cea.fr
Website:
http://www.virtuoso.eu/

Project objectives

The VIRTUOSO Project aims to provide an integrated open source information exploitation (OSINF) toolbox to European authorities working in border security. This toolbox will extend the "security distance" of Europe's borders by allowing EU agencies and member states to anticipate, identify and respond to strategic risks and threats in a timely manner. In short, the project aims to:

- » Improve the situational awareness of those organisations and individuals charged with securing Europe's borders;
- » Help anticipate risks such as terrorism, illegal migration and the trafficking of goods and people using OSINF;
- » Create the kernel of a pan-European technological platform for the collection, analysis and dissemination of open source information, thus ensuring greater interoperability among European actors involved in border security;
- » Provide the tools for crisis management response if anticipation fails or in the event of a rupture scenario.

Description of the work

The VIRTUOSO Project places considerable importance on the involvement of end-users. The project will be developed incrementally in response to their specific requirements.

During the first end-user requirements phase, a state-of-the-art set of tools will be demonstrated to help end-users better understand the utility of the VIRTUOSO toolkit.

Three versions of the VIRTUOSO Toolkit will be delivered:

- » *VIRTUOSO-V0:* A very basic version of the framework, integrating basic functions and demonstrating its potential;
- » *VIRTUOSO-V1:* A first version of the framework integrating some operational functions;
- » *VIRTUOSO-V2:* A second version of the framework with all operational functions adapted and/or developed.

Work Packages:

- » *WP0:* Management;
- » *WP1:* End-users requirements (10 workshops organised with end-users);
- » *WP2:* Architecture and infrastructure tools;
- » *WP3:* Privacy, ethical and legal aspects;
- » *WP4:* Data acquisition;
- » *WP5:* Processing;
- » *WP6:* Knowledge management;
- » *WP7:* Decision support and visualization;
- » *WP8:* Integration and demonstration;
- » *WP9:* End-Users validation (10 workshops organised with end-users);
- » *WP10:* Dissemination.

Expected results

This seamless OSINF platform will aggregate, in realtime, content from the internet, leading subscription providers, and broadcast media. This content will be filtered and analysed using text mining and other decision support technologies to improve situational awareness and provide early warning to end-users.

The project's deliverables include a demonstrator of the VIRTUOSO toolkit (one that integrates various information services and intelligence applications) and full documentation on the platform itself.

The core platform will be freely available as open source software at the end of the project.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST)	France
Defence and Security Systems (EADS)	France
Origin Sociedad Anonima Espanola (ATOS)	Spain
Mondeca SA (Mondeca)	France
Newstin a.s (NWT)	Czech Republic
SAIL Technology AG (SailLabs)	Austria
Aalborg University (AAU)	Denmark
Thales Communications (TCF)	France
Bertin Technologies (Bertin)	France
Stichting Katholieke Universiteit / Brabant Universiteit Van Tilburg (TILT)	The Netherlands
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Ingenieria de Sistemas Para la Defensa de Espana SA (Isdefe)	Spain
Hawk Associates Limited (HAWK)	United Kingdom
Eidgenössische Technische Hochschule Zürich (ETH Zurich)	Switzerland
Compagnie Europeenne d'Intelligence Strategique (CEIS)	France
Universita Degli Studi di Modena e Reggio Emilia (CRIS/UoM)	Italy
Columba Global Systems Ltd. (Columba)	Ireland
Thales Research and Technology (THALES)	France

AEROCEPTOR / UAV BASED INNOVATIVE MEANS FOR LAND AND SEA NON-COOPERATIVE VEHICLES STOP

© Jonoman1 Dreamstime.com

Information

Grant Agreement N°
285144
Total Cost
€4,839,873
EU Contribution
€3,468,859.75
Starting Date
01/01/2013
Duration
36 months

Coordinator

INSTITUTO NACIONAL DE TÉCNICA AEROESPACIAL (INTA)
Aeronautic Programs Department
Crtra Ajalvir km 4
28850
Torrejón de Ardoz, Madrid, Spain
Contact
Vicente de Frutos Cristóbal
Tel: +34 91 587 66 58
Fax: +34 91 520 16 16
E-mail: frutoscv@inta.es
Website: www.aeroceptor.eu

Project objectives

When approaching the problem of non-cooperative vehicles in Europe two different groups are in focus: land and sea vehicles (such as: motorbikes, cars, trucks and maritime boats). These vehicles are considered non-cooperative, when the Law Enforcement Agents are trying to stop them but the vehicle drivers do not obey the orders and signals of the agents. Maritime scenarios include the use of speedboats by organised crime groups for border crossing, drugs and weapons smuggling. Ground vehicles can be found also in a wide number of scenarios. These scenarios embrace situations ranging from routine traffic control attempts, to stolen or hijacked car pursuits, crime scene escapes and, the most complex ones, complicated and dangerous hostage situations. Law enforcement officers always seek for means to perform the stop and arrest procedure in the safest way for both the law enforcement officers, the offenders, and the rest of the people involved.

AEROCEPTOR project aims at increasing the capability of Law Enforcement Authorities (LEA) to remotely, safely and externally control and stop non-cooperative vehicles in both land and sea scenarios, by means of a Remote Piloted Aerial System (RPAS), the subset of Unmanned Aerial vehicles (UAV). Full consideration will be given to legal and human rights aspects, which are an integral part of the project. The scenarios will moreover be audited from the ethics point of view before their implementation.

RPAS consists of an aerial vehicle that is remotely piloted. This solution has several advantages, such as:

» Higher security level for law enforcement agents and lower error rate;

» Increasing the efficiency and effectiveness of interception operations, since RPAS are quickly deployable and have an all-weather and 24/7 operation capability;

» Decreasing the risk of human overreaction in interception operations;

» Offering a cost effective and environmentally friendlier solution due to their reduced weight and therefore less fuel consumption;

» and last but not least, being humans still the best decision makers, RPAS offers a solution able to combine the human capability for decision making with a high automated operation capability owing to the continuous monitoring of the operation and fulfilling "state of the art " privacy respect legal requirement.

Description of the work

The project will cover different types of activities:

1. Research and Technological Development activities:

» Electromagnetic jamming payload equipment development;

» Development of an innovative RPAS control system;

» Technological development to adapt existing payloads

2. Systems engineering activities to integrate the different subsystems, technologies, new developments and Components Off The Shelf (COTS) into the new system.

3. Legislation and regulatory assessment activities, to study the needed regulatory framework allowing this kind of RPAS to operate (certification and integration into aerospace).

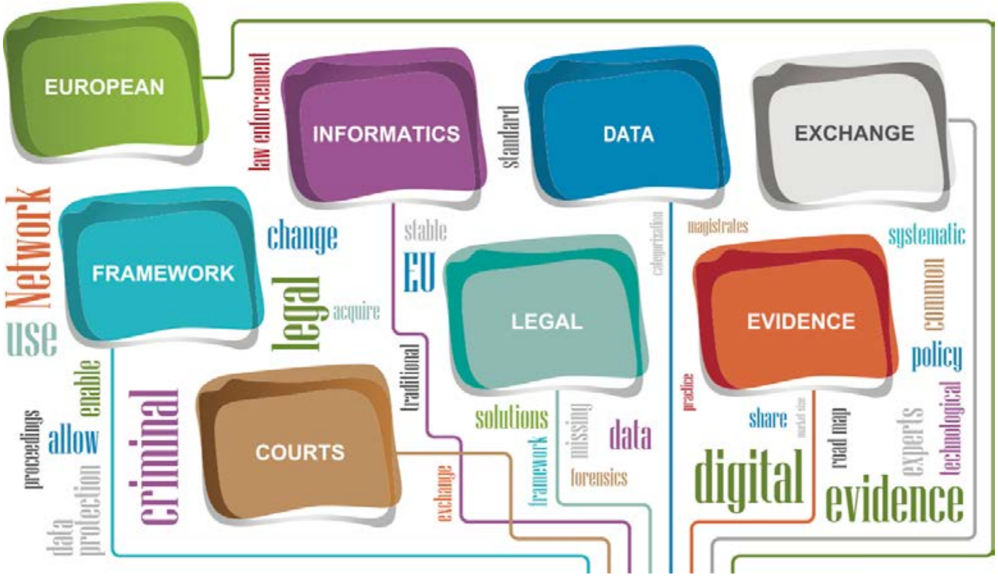
4. Safety, Security and ethical issues assessment, in order to ensure that the proposed system complies with the necessary safety and security levels and is compliant with the European regulations.

Expected results

Interception of non-cooperative vehicles by law enforcement agencies is often a very dangerous task. Accident may occur that threatens the lives of those who intercept, for example the police or border guards. At the same time it can also result in the loss of life of the offenders, which is of course not intended. Moreover, often innocent third parties are involved in accidents occurring in vehicular pursuits, that is, people who just happen to stand or pass by. That's the reason why current interception means are neither safe nor effective. I. AEROCEPTOR will develop a concept that will increase effectiveness and safety of these procedures, enhancing also the capability range by developing a technology that will allow LEAs to monitor, track and stop land and maritime non cooperative vehicles owing to an automated aerial system.

PARTNERS	COUNTRY
Instituto Nacional de Técnica Aeroespacial (INTA)	Spain
Ingeniera de Sistemas para la Defensa de España SA (ISDEFE)	Spain
Aerospace and Defence SAU (GMV)	Spain
Office National d'Etudes et de Recherches Aerospatiales (ONERA)	France
Przemyslowy Instytut Automatyki i Pomiarow piap (PIAP)	Poland
Alma Mater Studiorum-Universita di Bologna (UNIBO)	Italy
Austrian Institute of Technology GMBH (AIT)	Austria
Israel Aerospace Industries LTD. (IAI)	Israel
Turk Otomobil Fabrikasi Anonim Sirketi (TOFAS)	Turkey
Sigmund Freud Privatuniversitat Wien GMBH (SFU)	Austria
Ministerio del Interior (MIR)	Spain
Rotem Technological Solutions LTD (ROTEM)	Israel
Etienne Lacroix Tous Artifices SA (LACROIX)	France
Ministry of Public Security (MOPS/INP)	Israel
Zabala Innovation Consulting, SA (ZABALA)	Spain

EVIDENCE / European Informatics Data Exchange Framework for Courts and Evidence



Information

Grant Agreement N°
608185
Total Cost
€2,303,648
EU Contribution
€1,924,589
Starting Date
01/03/2014
Duration
32 months

Coordinator

CONSIGLIO NAZIONALE DELLE RICERCHE - NATIONAL RESEARCH COUNCIL OF ITALY (CNR-ITTIG)
Institute of Legal Information Theory and Techniques of the National Research Council of Italy (ITTIG)
Via De' Barucci 20
50127 - Florence- Italy
Contact
Maria Angela Biasiotti
Tel: +39 055 4399683
Mobile: +39 3393511657
Fax: +39 055 4399605
E-mail: mariangela.biasiotti@ittig.cnr.it
Website: www.ittig.cnr.it

Project objectives

EVIDENCE aims to provide a roadmap for the systematic and uniform application of new technologies in the collection, use and exchange of evidence. This will incorporate standardised solutions to create efficient regulation, treatment and exchange of digital evidence for law enforcement agencies (LEAs), judges, prosecutors and lawyers in the criminal field. This should lead to a common european framework to gather, use and exchange digital evidence (e-evidence) according to common standards and rules.

To produce the roadmap the following objectives are considered essential:

» Development of a common and shared understanding of what electronic evidence is, and the relevant concepts of electronic evidence in involved domains and related fields (digital forensics, criminal law, criminal procedure, criminal international cooperation);

» Understanding of which rules and criteria are utilised for processing electronic evidence in EU Member States, and how the exchange of evidence is regulated;

» •Identification of the criteria and standards necessary for guaranteeing reliability, integrity and chain of custody required for electronic evidence in the EU and eventually its exchange across borders;

» Definition of operational and ethical implications for LEAs all over Europe;

» Identification and development of technological functionalities for a common European framework in gathering and exchanging electronic evidence.

Description of the work

EVIDENCE has several research work packages, each led by an experienced project member responsible for clearly delineated, measurable deliverables. The packages represent four distinct work streams which build on and inform each other:

» Status Quo Analysis (WP2, WP3, WP4, WP6, WP8),

» Technical Functionalities development (WP5),

» Impact and Testing (WP5, WP7), and

» Road Map (WP9).

Results

The Evidence Project has developed its common and shared understanding of what electronic evidence is and the relevant concepts. An EVIDENCE categorisation, based on its own definition of electronic evidence, has created and is now available online.

Based on a pilot comparative study, the results suggest there is no comprehensive international or European legal framework relating to e-evidence. Although some regulations exist at national level, rules vary considerably.

The work on legal issues also produced an overview of the existing situation regarding the criteria of data protection and privacy rules when digital evidence is exchanged. As for the exchange process there are no published standards. According to our information gathered so far, it seems that in cross-borders criminal cases, cooperation is mostly based upon international agreement. This approach is similar across countries and, at first glance, does not appear based on any electronic means at all.

The project's standards work for the handling of e-evidence has allowed us to build up an online Digital Forensics Tools Catalogue comprising over 1,200 different tools devoted to Acquisition and Analysis processes.

Remarks:

These mid-terms results suggest that the way forward for the electronic evidence exchange within the EU would be to introduce an "environment" comprised of both legal and technical requirements to be used by judicial and police authorities, and by private stakeholders. This would speed up the process, optimise costs, and foster cooperation and trust among the involved competent authorities.

The EVIDENCE roadmap will greatly impact on the existing scenario by:

- positively influencing judges, who are the key actors in admitting electronic evidence, and police experts who gather such evidence;
- aiding in the adjustment and/or creation of national and supranational legislation;
- enhancing confidence in the collection, analysis and conservation of electronic evidence;
- improving communication between the actors related to electronic evidence, at the national, European and international level;

PARTNERS	COUNTRY
Consiglio Nazionale delle Ricerche (CNR-ITTIG and CNR-IRPPS)	Italy
Rijksuniversiteit Groningen (RUG)	The Netherlands
International Criminal Police Organization (Interpol)	France
Leibniz Universität Hannover (LUH)	Germany
Laboratorio di Scienze della Cittadinanza (LSC)	Italy
Universita ta Malta (UoM)	Malta
Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)	Belgium
Law and Internet Foundation (LIF)	Bulgaria
Conseil des Barreaux Européens AISBL (CCBE)	Belgium

LINKSCH / Grasping the Links in the Chain: Understanding the Unintended Consequences of International Counter-Narcotics Measures for the EU

© selimaksan - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285073
Total Cost
€1,067,166.80
EU Contribution
€881,742.20
Starting Date
01/02/2012
End Date
31/01/2015

Coordinator

UNIVERSITY OF GLASGOW
School of Humanities
2 University Gardens
Glasgow University
G12 8QQ Glasgow,
United Kingdom
Contact
Alexander Graham Marshall
Tel: +44 141 330 8581
Mobile: +44 07501986739
Fax: +44 141 330 5000
E-mail: alexander.marshall@glasgow.ac.uk

Project objectives

- design a model of current market dynamics along key illicit commodity chains that currently affect the EU;
- arrive at a typology of unintended consequences generated by current policy as it interfaces at numerous points along these two chains, taking into account both national and international efforts at control and prohibition;
- investigate via empirical investigation (fieldwork) the actual scale and nature of the most harmful of these unintended consequences, with a view to generating policy recommendations for improving them;
- and disseminate the results of this research to a wide variety of key audiences in fora that will also accommodate comparative data from studies of related areas (the cocaine trade for example).

Description of the work

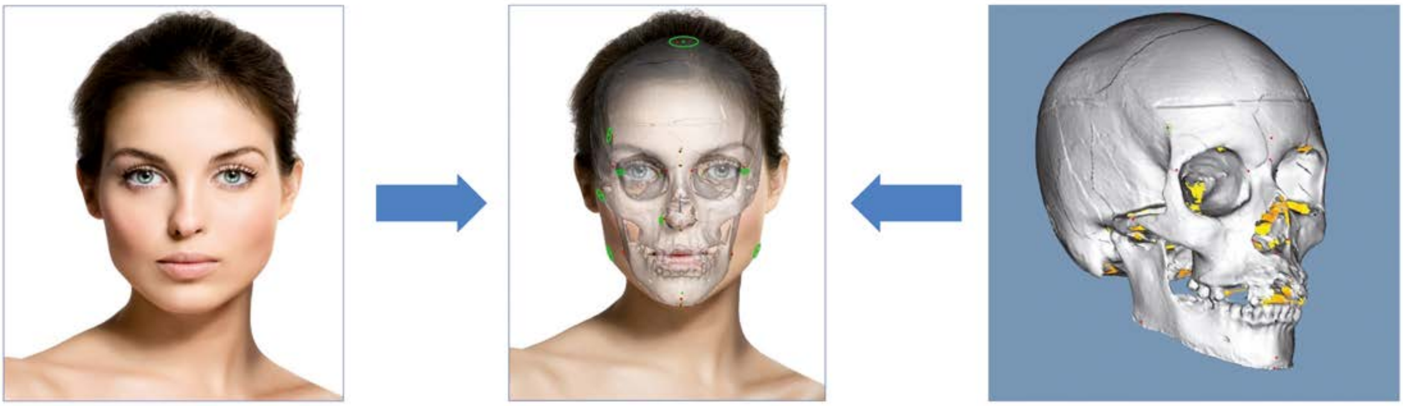
This project aimed to develop a model of unintended consequences utilizing the conceptual prisms of global commodity chain theory and hybrid political regimes, and treating the current prohibition regime as a hybrid political system running from closed to open access orders. This process incorporated both a survey and summary of current state of the art thinking on unintended consequences of the contemporary prohibition regime, and a series of clearly targeted research questions which were pursued in active fieldwork across Morocco, Turkey, Russia, Afghanistan and Kazakhstan. Audiences to be engaged with during this process included NGOs, international agencies, government bodies and local communities. The work was novel in the manner that seeked to compare the soft and the hard end of the illicit drug spectrum and to look at policy activities beyond the immediately obvious ones of prohibition and harm reduction.

Results

Regarding the unintended consequences of drug policy for countries connected with EU illicit drug consumption (hashish from Morocco, heroin from Afghanistan), the LINKSCH project produced a 169,000-word final report. This included 17 specific policy recommendations, 3 suggestions for further funded research, alongside (to date) four published articles disseminating the work of the consortium, a major dissemination conference in Brussels in 2014 and a project website for analysis and discussion. Further books and articles from the LINKSCH project are expected for the future.

PARTNERS	COUNTRY
University of Glasgow (UGLA)	United Kingdom
Virtual Hand Research (VHR)	The Netherlands
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNRS)	France
Coventry University (CBS)	United Kingdom
SCHOOL OF ORIENTAL AND AFRICAN STUDIES, UNIVERSITY OF LONDON (SOAS)	United Kingdom
THORNLEY MANSFIELD LTD (MANSF)	United Kingdom
UNIVERSITAET POTSDAM (POTSDAM)	Germany

MEPROCS / New methodologies and protocols of forensic identification by craniofacial superimposition



Information

Grant Agreement N°
285624
Total Cost
€1,199,750
EU Contribution
€1,005,800
Starting Date
01/02/2012
Duration
24 months

Coordinator

Fundación para el Progreso del Soft Computing (ECSC)
Applications of Fuzzy Logic and Evolutionary Algorithms Research Unit
C/ Gonzalo Gutiérrez Quirós, s/n
33600, Mieres, Asturias, Spain
Contact
Sergio Damas Arroyo
Tel: +34 985 45 65 45
Fax: +34 985 45 66 99
E-mail: sergio.damas@softcomputing.es
Website: www.meprocs.eu

Project objectives

The MEPROCS project aims to propose a common EU framework to allow the extensive application of the craniofacial superimposition (CS) technique in practical forensic identification scenarios commonly tackled by European scientific police units.

This framework will include:

» the implementation of an existing semi-automatic method to assist the forensic experts in the application of the CS technique, resulting in a simple, quick, and systematic approach;

» the definition of standard protocols at European level, leading to the objective application of the CS technique in different forensic identification scenarios; and

» the specification of a forensic science methodology to provide an objective evaluation of the forensic identification results achieved by CS, avoiding particular assumptions that could bias the process. Hence, the project clearly promotes the validation and exchange of CS protocols and methodologies among different organisations.

Description of the work

1. Analysis of the existing methods and procedures in the field of CS-based forensic identification.
A review of the state of the art in forensic identification from skeletal remains by CS will be addressed, identifying all the reported applications of the CS technique, including materials, protocols, methods and tools used.

2. Consolidation of the network.
Engage new stakeholders by contacting the most representative forensic anthropology labs, researchers, and end-users, in order to expand the implementation of the network and widen its scope.

3. Establishment of specific protocols for the application of CS to different scenarios.
Identify the different scenarios where CS has been applied, reporting common problems, number of tackled and solved cases, predominant scenarios and reliability. Advantages and disadvantages of the different procedures followed by the end-users in the network will be discussed. Standard protocols for each kind of scenario (missing people, mass disasters, etc.) will be defined.

4. Specification of validation techniques.
Study previous approaches to propose semi-automatic methods to asses CS results. Special focus will be placed on analysing ethical and legal issues concerning scientific use of identification cases. Finally, the robustness and accuracy of the automatic CS method will be assessed through experiments over all the identification cases available.

5. Global CS forensic identification framework definition.
Design of a CS-based methodological framework that can be easily distributed and accessed by stakeholders, and evaluation of its performance.

6. Dissemination and training.

We will work on improving communication between the different communities involved. Events to train end-users in the proposed automatic CS-based forensic identification framework will be organised. The visibility of the project results will be promoted, and a handbook on the CS identification framework published.

Expected results

- Definition of standard protocols for the application of CS to different scenarios;
- Specification of objective and automatic validation techniques for the CS identification results
- Promotion of the application of the resulting CS-based forensic identification methodological framework
- Enhancement of the cooperation among forensic anthropologists, technical researchers, and end-users
- Enhancement of the CS forensic identification technique

PARTNERS	COUNTRY
European Centre for Soft Computing - ECSC	Spain
Consorci di Ricerca Sistemi ad Agenti - CORISA	Italy
European Council of Legal Medicine - ECLM	Portugal
University of Granada - UGR	Spain
Israel National Police (Ministry of Public Security) - INP	Israel
Forensic Sciences Centre (Universidade de Coimbra) - FSC	Portugal
Guardia Civil (Ministerio del Interior) - GC	Spain

MIDAS / The development and validation of a rapid millifluidic DNA analysis system for forensic casework samples

© rolffimages - Fotolia.com

Information

Grant Agreement N°
242345
Total Cost
€4,688,674.80
EU Contribution
€3,231,404.60
Starting Date
01/09/2010
Duration
36 months

Coordinator

FORENSIC SCIENCE SERVICE LTD
Research and Development
Birmingham Business Park,
Solihull Parkway
B37 7YN
United Kingdom
Contact
Cecilia Buffery
Tel.: +44 1256771521
Mobile: +44 7824 434158
Fax: +44 1256771521
E-mail: Cecilia.buffery@fss.pnn.police.uk
Website: www.forensic.gov.uk

Project objectives

The objective of the project is to specify and develop a working instrument for the rapid analysis of DNA from samples recovered from a scene of crime. The system will be simple to use and require a single input from the user. The system will be "closed" and will operate on a fully automated basis such that a sample is simply introduced into the instrument and no further sample manipulation is required from the individual. The development of a closed system for the DNA as described above brings a number of advantages to the field of forensic science.

The core scientific and technical objectives of MiDAS are therefore to:

- Develop an agreed technical specification for the instrument and consumables;
- Deliver a prototype integrated instrument for validation;
- Evaluate the instrument in accordance with the validation plan and user requirement;
- Evaluate the instrument and cartridge designs to ensure they are fit for manufacture;
- Evaluate the legal requirements for sample handling and data transfer and protection;
- Determine system validation strategies for each of the participant member states.

Description of the work

Work Package 1 – Technical Specification

Define and agree the specification for a cartridge-based fully integrated millifluidic device for forensic DNA analysis. Calling on all project participants to draw on their own fields of expertise, WP1 will ensure the system is defined so as to fulfil internationally agreed guidelines for the analysis of DNA in a forensic context.

Work Package 2 – Prototype development

Develop and evaluate the prototype DNA analysis device. The instrument will be developed to meet the technical specifications as defined by the Technical Specification Board (TSB) in WP1 and tested against the agreed acceptance criteria. Any optimisation of the final system will take place here and implemented changes will be re-evaluated.

Work Package 3 – Instrument and software validation

Validate the prototype instrument delivered from WP2 in accordance with the validation plan delivered in WP1.

Work Package 4 – Process Integration

Define the process whereby the instrument is integrated into the forensic organisation and how it will integrate with current processes. An understanding of the technological, organisational and human implications of implementation will allow an assessment of the impact to be made.

Work Package 5 – System Validation & Implementation

Define, agree and deliver the system validation. This process is likely to be different in different jurisdictions. It is essential therefore to incorporate knowledge from all the end user partners in the consortium and to identify those parties interested in early implementation of the instrument to their own process.

Work Package 6 – Data Protection

Define, agree and deliver the Data Protection required by the project to industry standards and EU guidelines.

Work Package 7 – Device and System Scalability

Produce a number of strategic plans to allow the device to be developed allowing it to be commercially viable and to consider manufacturability.

Work Packages 8 and 9 – Dissemination and Exploitation; Project Management

Work Package 8 (Dissemination & Exploitation) together with Work Package 9 (Project Management and Reporting to the EC) will ensure effective project management and communication with the EC.

Work in WP8 will also evaluate the impact the successful implementation of a rapid DNA analysis system might have on society as a whole.

Expected results

MiDAS will deliver simple to operate automated DNA analysis technology and will validate this technology and associated processes required for its implementation, enabling forensic DNA analysis to be carried out at the crime scene. With fast results authorities will have the opportunity to rapidly compare the scene samples against DNA profiles from known criminals or results from other crime scenes held in national DNA databases. The project will have dramatic implications for both criminal justice and international security, with the ability to deliver vital intelligence results much more quickly both in a national sense and across the EU.

PARTNERS	COUNTRY
Forensic Science Service Ltd (FSS)	United Kingdom
Grid Xitek Limited (GXD)	United Kingdom
Medizinische Universitaet Innsbruck (IMU)	Austria
Bundeskriminalamt (BKA)	Germany
Netherlands Forensic Institute (NFI)	The Netherlands
Arizona Board of Regents (University of Arizona- UoA)	United States

ODYSSEY / Strategic pan-European ballistics intelligence platform for combating organised crime and terrorism

© Dwight Davis - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218237
Total Cost
€3,848,383.54
EU Contribution
€2,395,000
Starting Date
01/11/2008
End date
30/04/2011

Coordinator

SHEFFIELD HALLAM UNIVERSITY
Howard Street
UK - S1 1WB Sheffield
United Kingdom
Contact
Professor B. Akhgar
Tel: +44 (0) 114 225 6770
Fax: +44 (0) 114 225 6931
E-mail: b.akhgar@shu.ac.uk
Website:
www.odyssey-project.eu

Project objectives

The ODYSSEY project undertook to research and develop a secure platform for the sharing of information about gun-crime throughout the EU.

The main project objectives were:

» creation of European standards for ballistics data collection, storage and sharing;

» demonstration of a secure, interoperable platform for the management of crime information and the sharing of ballistic intelligence;

» development of techniques for the mining of data and extraction of knowledge about gun crime across the EU;

» exploitation of automated and semi-automated processing and analysis of crime data to generate 'red flags' and analysis of complex data with multiple reference models;

» improved mutual co-operation, security and sustainability across the EU.

Results

The ODYSSEY project established that sharing data about gun crime between authorities and jurisdictions is technically feasible, and would bring operational benefits. These benefits would arise from the creation of trans-national data sets that could be manipulated using advanced data mining techniques to reveal hitherto hidden information.

The bedrock of these findings was the creation of a potential set of new EU standards for gun crime data defined by their own data structures, taxonomies and ontologies. These can now be taken onward to CEN, one of the EU's technical standards organisations, or ISO for evaluation and use.

A working prototype – an automated interoperable platform for data sharing – was also tested. It consisted of a secure platform for the management of crime information and the sharing of ballistics intelligence. It was tested to assess its ability to provide analysis, situation awareness and threat monitoring functionality. This was supported by a distributed technological infrastructure to store metadata in a semantic format for advanced querying and analysis.

As well as demonstrating automated 'red flag' functions, the tests also highlighted the possibility of expanding such a secure platform into other forensic areas such as DNA, fingerprints and physical evidence and other cross border policing domains such as human trafficking.

Odyssey thus demonstrated through its prototype the potential for a federated system to provide cost and time savings, as compared to current cross-EU processes.

PARTNERS	COUNTRY
SHEFFIELD HALLAM UNIVERSITY (SHU)	United Kingdom
AN GARDA SIOCHANA (AGS)	Ireland
ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA (Atos)	Spain
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
EUROPEAN POLICE OFFICE (EUR)	The Netherlands
FORENSIC PATHWAYS LIMITED (FPL)	United Kingdom
MINISTERIO DELL'INTERNO (DAC)	Italy
MIP - CONSORZIO PER L'INNOVAZIONE NELLA GESTIONE DELLE IMPRESE E DELLA PUBBLICA AMMINISTRAZIONE (MIP)	Italy
North Yorkshire Police Authority (North Yorkshire Police)	United Kingdom
SAS SOFTWARE LIMITED (SAS)	United Kingdom
SESA - COMMERCE HANDELSGMBH (SESA)	Austria
WEST MIDLANDS POLICE AUTHORITY (WMP)	United Kingdom
XLAB RAZVOJ PROGRAMSKE OPREME IN SVETOVANJE D.O.O. (XLAB)	Slovenia

SAVELEC / Safe control of non-cooperative vehicles through electromagnetic means

© SAVELEC

Information

Grant Agreement N°
285202
Total Cost
€4,253,993
EU Contribution
€3,321,749
Starting Date
01/01/2012
Duration
40 months

Coordinator

INSTITUTO DE APLICACIONES DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES AVANZADAS
Advanced Projects and Testing Area
Camino de Vera s/n
46022 Valencia, Spain
Contact
Francisco Javier Díaz Jiménez
Tel: +34 963 877 278
Mobile: +34 963 877 278
Fax: +34 963 877 279
E-mail:
francisco-javier.diaz@itaca-ct.es
Website:
www.savelec-project.eu

Project objectives

SAVELEC aims to provide a solution for the external and safe control of a non-cooperative vehicle with no consequences for the persons inside the vehicle or other persons and objects nearby. The proposed solution is based on the use of electromagnetic means in order to disrupt the correct functioning of the electronic components inside the vehicle, which will make it slow down and stop. The SAVELEC approach is based on the premise of obtaining an optimized solution in terms of field strength, ensuring the solution complies with EU guidelines regarding human exposure to electromagnetic fields.

The ultimate purpose of the project is to design and build a car-stopper prototype to validate the technology. A real demonstration on cars going along a controlled track will be performed to assess the technology in a realistic scenario.

The involvement of security forces as end-users in the project is a key factor as regards the need to have realistic information about the use-cases, scenarios and operational parameters.

SAVELEC will propose a regulatory framework regarding the use of the technology by EU security bodies in their daily missions.

Description of the work

The work programme will start with an assessment of the use-cases and scenarios that will lead to the definition of a set of operational requirements. These activities will be performed in close cooperation with the end-user panel made up of a group of security bodies from Spain, France, Germany and Greece.

An in-depth technology review of the available state-of-the-art technology that may be considered as a reference to follow for generating the signals needed for the project's activities will be performed afterwards. This will consist of waveform generation and modulation, high-power amplifiers, power sources and ultra directional radiating elements, high bandwidth and the ability to withstand high-power signals. In addition, a series of activities are planned to review the electronic architectures and systems in cars and light commercial vehicles, providing a list of vulnerabilities regarding electromagnetic coupling effects ranked according to their expected effectiveness for the following test bench experiments.

The test bench experiments will consist of defining, designing and building automotive test bench architecture for electrical measurements. Additionally, a specific set-up for generating a wide range of electromagnetic signals will be prepared. These two elements will be used to perform a wide range of EMC experiments on sensors, electronics, wires and communications in order to identify the optimized type of signal that could lead to stopping the car as a consequence of the electromagnetic coupling.

Some additional considerations of more legal and safety aspects will be evaluated in the scope of collateral effects regarding the use of this kind of electromagnetic means: human exposure to electromagnetic fields (user, target and persons in close proximity), explosive atmosphere exposure to electromagnetic fields and an assessment of the drivers' reaction once the car goes into abnormal behaviour mode. In addition to this, specific legal and ethical studies will be carried out regarding the use of this kind of electromagnetic means by security forces. A regulatory framework will be sketched out and proposed.

Taking into consideration all the aforementioned outcomes, a breadboard-level prototype car-stopper device will be designed, manufactured and validated in an operational environment.

Expected results

SAVELEC will make technology available that could be used by law enforcement agencies in their daily missions to stop and control non-cooperative land vehicles at distance, safeguarding all the legal and ethical considerations that may arise from the use of this kind of technology. An extrapolation to the case of maritime missions could follow.

SAVELEC will demonstrate the new technology's added value to law enforcement agencies as regards their daily operations. The project will raise awareness among policy-makers and help develop the proper legal framework.

PARTNERS	COUNTRY
INSTITUTO DE APLICACIONES DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LAS COMUNICACIONES AVANZADAS (ITACA)	Spain
DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV (DLR)	Germany
MBDA FRANCE SAS (MBDA)	France
IMST GMBH (IMST)	Germany
TECHNOLOGICAL EDUCATIONAL INSTITUTE OF PIRAEUS (TEIP)	Greece
BCB INFORMÁTICA Y CONTROL S.L. (BCB)	Spain
STATENS VAG- OCH TRANSPORTFORSKNINGSINSTITUT (VTI)	Sweden
OTTO-VON-GUERICKE-UNIVERSITAET MAGDEBURG (OVGU)	Germany
AKADEMIA OZBROJENYCH SIL GENERALA MILANA RASTISLAVA STEFANIKA (AOS)	Slovakia
HELLENIC AEROSPACE INDUSTRY SA (HAI)	Greece

SMARTPRO / Lightweight, flexible and smart protective clothing for law enforcement personnel

Information

Grant Agreement N°
607295
Total Cost
€3,777,451.27
EU Contribution
€2,741,826.52
Starting Date
01/04/2014
Duration
42 months

Coordinator

MATERIALS INDUSTRIAL RESEARCH AND TECHNOLOGY CENTER S.A. (MIRTEC)
R&D – Athens Branch
Eleftheriou Venizelou 4
176 76, Kallithea, Athens,
Greece
Contact
Silvia Pavlidou
Tel: +30 210 9234932
Mobile: +30 6944639248
Fax: +30 210 9235603
E-mail:
s.pavlidou@ebetam.gr
Website: www.ebetam.gr

Project objectives

The concept of SMARTPRO lies in the development of lightweight and flexible protective clothing, incorporating smart functionalities and designated for law enforcement authorities.

Modern body armours still have some of the same drawbacks as the old ones, as they are mostly heavy, bulky and rigid. They limit the wearer's mobility and agility and are impractical for use on joints, arms, legs, etc. Also, body armours have traditionally been designed to protect the wearer against ballistic threats and, thus, they provide only a limited level of protection against knives, sharp blades or sharp-tipped weapons.

Recent studies reveal that stab and puncture have become a main cause of police officers' injuries. There is an obvious need to develop materials that combine stab and ballistic protection, while retaining their flexibility and low weight.

Description of the work

The work in SMARTPRO addresses the following:

» Development of optimized protective (ballistic/ stab resistant) textile and composite structures, including woven and 3D knitted textiles structures, fish scale-type composites and innovative hybrid structures made of synthetic polymer nanofiber composites.

» Development and application of innovative surface treatments aiming to improve textiles performance on an areal density basis. These include surface application of shear thickening fluids, ceramic coatings, dilatant powders, carbide nanoparticles and cross-linkable side-functionalized aromatic polymers.

» Optimized assembly of the protective panel aiming to achieve maximum protection at minimum weight and cost.

» Development and integration of smart systems, including wearable GPS, electrocardiogram, temperature and gas sensors.

» Ergonomic design of the body armour, considering also modularity.

» Prototypes development.

Expected results

The project is expected to lead to new body armours and protective gear for body parts other than the torso, characterized by low weight and increased flexibility and incorporating smart functionalities that may increase awareness of law enforcement personnel. The new PPE will be ergonomically designed, take into account the importance of modularity, and is expected to find wide acceptance by the end-users.

PARTNERS	COUNTRY
European Commission (EC)	Belgium
Materials Industrial Research and Technology Center S.A. (MIRTEC)	Greece
Acondicionamiento Tarrasense Associacion (LEITAT)	Spain
Next Technology Tecnotessile Società Nazionale di Ricerca r.l. (NTT)	Italy
Foundation for Research and Technology Hellas (FORTH)	Greece
Kostas Siamidis AE (SIAMIDIS)	Greece
Rheinisch-Westfaelische Technische Hochschule Aachen (RWTH)	Germany
B.C.B International Limited (BCB International Lt)	United Kingdom
Soliani EMC SRL (SOLIANI)	Italy
E. CIMA SA (CIMA)	Spain
Departament d’Interior - Generalitat de Catalunya (INT)	Spain

CAPER / Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime

© Louise Gagnon - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261712
Total Cost
€7,143,920.80
EU Contribution
€5,579,346
Starting Date
01/07/2011
End Date
31/10/2014

Coordinator

S21SEC INFORMATION SECURITY LABS S.L.
R&D
Parque empresarial la Muga, 11 1a planta
31160 Orkoien
Spain
Contact
Carlos MONREAL
Tel: +34948100013
Mobile: +34 607 370 017
Fax: +34948336930
E-mail:
cmonreal@s21sec.com
Website: www.s21sec.com/

Project objectives

The goal of the CAPER project was to create a common platform for the prevention of organised crime through sharing, exploitation and analysis of information sources. CAPER supported collaborative multilingual analysis of audiovisual content (video, audio, speech and images) and biometrics information, supported by Visual Analytics and Data Mining technologies. The integration of database technologies, application workflow and semantic modelling of processes, and legal and privacy limitations, permitted participating Law Enforcement Authorities (LEA) to share information and investigative and experiential knowledge. The CAPER platform was built in close collaboration with the LEA users in order to fulfil their current and forthcoming needs. The project was clearly focused on the fusion and real validation of the existing state of the art, coupled with innovative new technologies, to solve current bottlenecks faced by LEAs.

Description of the work

The CAPER platform consisted of six core elements:

Open and Closed Data Sources: Multi-format, multimedia and multimodal information from open sources, TV and Radio capture, and information in closed legacy systems are the data sources to be mined and evaluated by CAPER.

Data Acquisition: Depending on the information source type, different acquisition patterns were applied to ensure acquired information as a suitable format for analysis.

Information Analysis: Each analysis module was geared towards a specific content type, i.e. text, image, video, audio and speech or biometric data.

Information and Reference Repositories: Both source data when required, and the information mined by the information analysis modules, were stored in these repositories, separated by content type.

Interoperability and Management Application: This was the end users' workbench. Built on a web based collaborative platform, it allowed the Law Enforcement Officers to create and configure their monitoring requests and analysis petitions.

Visual Analytics (VA) and Data Mining (DM): Grouped under the management application, the VA and DM elements were key components of the CAPER platform, since they provided the intelligence necessary to support the outputs of the system.

Results

CAPER created a notable cooperative atmosphere in which technical staff and LEAs can work in the same direction. In the workshops organized, LEAs shared their expertise and knowledge with the rest of the consortium and generated a fruitful network, resulting from helpful cooperation during the project. The platform developed in CAPER captures a wide range of information types from open sources, analyzing and presenting it by a set of visualization tools. Specifically, it is able to collect vast amounts of data in different formats (texts, images, audios and videos) from publicly available sources, such as Web and social media networks. Then, it analyzes these datasets, applying a semantic analysis and transforming them into a knowledge repository that can be exploited by a set of graphic tools to be visualized by information analysts. In support to the technology development, the ethical analysis contributed to the creation and implementation of a regulatory model which is a new, practical and plausible ethical and legal framework for security projects and for users' data protection.

PARTNERS	COUNTRY
S21Sec Information Security Labs S.L. (S21sec)	Spain
Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones Vicomtech (VICOM)	Spain
Fraunhofer – Gesellschaft zur Foerderung der Angewandt (Fraunhofer-IGD)	Germany
Synthema (Synthema)	Italy
VOICEINTERACTION – Tecnologias de Processamento de Fala, S.A. (VI)	Portugal
ALTIC	France
Technion – Israel Institute of Technology (Technion)	Israel
Angel Iglesias S.A.- IKUSI (IKUSI)	Spain
Alma Consulting Group SAS (Alma)	France
Consiglio Nazionale Delle Ricerche - Institute for Informatics and Telematica (IIT)	Italy
Universitat Autonoma de Barcelona (UAB)	Spain
Studio Professionale Associato a Baker & McKenzie (BAK)	Italy
Ministero dell'Interno - Servizio Polizia Postale e delle Comunicazioni (Postal and Communications Police Service) (PCPS)	Italy
Serviciul de Informații Externe (External Intelligence Service) (SIE)	Romania
Polìcia Judiciària (Judicial Police) (PJ)	Portugal
Guardia Civil (Civil Guard) (GC)	Spain

CONPHIRMER / Counterfeit Pharmaceuticals Interception using Radiofrequency Methods in Realtime

© Elena Aliaga - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261670
Total Cost
€3,599,540
EU Contribution
€2,634,489
Starting Date
01/07/2011
End Date
31/12/2014

Coordinator

KING'S COLLEGE LONDON
Engineering
Strand
WC2R 2LS London
United Kingdom
Contact
Kaspar Althoefer
Tel: +44 (0)20 7848 2431
Mobile: +44 (0)77 888 7 555 3
Fax: +44 (0)20 7848 2932
E-mail: k.althoefer@kcl.ac.uk
Website: www.conphirmer.eu

Project objectives

The members of the CONPHIRMER consortium had come together to create a portable and easy-to-use sensor for telling genuine medicines from fakes, which customs officers and other agents of law enforcement could use without having to remove the medicines from their packaging. With this device agencies charged with tackling the growing menace of the trafficking in counterfeit medicines were able to screen packaged pharmaceuticals at EU borders and airports quickly and accurately, using a non-invasive and non-destructive technology that uses only harmless radio waves.

Description of the work

The consortium utilized a form of radio frequency spectroscopy known as Quadrupole Resonance (QR). This technology has been developed and deployed for the detection of concealed explosives and landmines and is considered human safe.

QR is a radiofrequency (RF) spectroscopic technique that can detect signals through multiple layers of cardboard, glass, plastic and/or wood. QR can analyse any compound containing a quadrupolar nucleus, which accounts for over 50% of elements in the periodic table, and, in particular, it is ideally suited for the analysis of compounds containing nitrogen, chlorine or bromine, sodium and potassium, which includes over 80% of all drugs.

The consortium developed a portable QR-based medicines authentication device tailored to the needs of customs officers operating at EU borders in parallel with identifying the QR characteristics of medicines that afford the best discrimination between real and fake medicines. QR "fingerprints" based on these key characteristics were put together to form a database that was of use not only on the CONPHIRMER device, but in all analytical applications of QR for medicines authentication.

Results

Successful field trials took place during 24 – 28 November 2014 at a postal sorting facility near Warsaw Chopin Airport, in Warsaw, Poland. The tangible outputs from the project are:

A method for generating a quadrupole resonance (QR) fingerprint designed to add a new dimension to the specificity and security of pharmaceutical packaging labelling, adding chemical information about the medicine itself to the labelling, ensuring that its contents are secured, not just the packaging.

A portable QR-based medicines authentication device. This device allows customs officers and others to test postal packages to ensure the actual medicines' content matches that stated on the CN22 without the need to remove the medicines from their packaging; and the ability to do this on site, at sorting offices and/or border posts.

An RF transducer for QR-based medicines authentication. This transducer has been designed specifically for use in authenticating packaged medicines with a configuration matched to typical medicines packet forms. The radiofrequency field projected by the transducer is manipulated in such a way as to penetrate the packets to reach the medicines within.

PARTNERS	COUNTRY
King's College London (KCL)	United Kingdom
French-German Research Institute of Saint-Louis (ISL)	France/Germany
University of Ljubljana (IMFM)	Slovenia
Jožef Stefan International Postgraduate School (IPS)	Slovenia
University of Lund (ULund)	Sweden
Rapiscan Systems Ltd (RSL)	United Kingdom
Polish Customs Service (PCS)	Poland
Stelar SRL (STELAR)	Italy
London South Bank University (LSBU)	United Kingdom
Bagtronics Ltd. (BAG)	United Kingdom

CUSTOM / Drugs and precursor sensing by complementing low cost multiple techniques

© morbyte - Fotolia.com

Information

Grant Agreement N°
242387
Total Cost
€5,295,523
EU Contribution
€3,486,406
Starting Date
01/06/2010
Duration
36 months

Coordinator

SELEX SISTEMI INTEGRATI S.P.A.
Contact
Anna Maria Fiorello
Tel: + 39 06 4150 3104
Mobile: + 39 3351379733
E-mail:
afiorello@selex-si.com
Website: www.selex-si.com

Project objectives

The project aims to develop a chemical sensor able to perform chemical identifications in contexts such as customs offices, where inspection of trucks, cars, containers, as well as people and baggage is required, in order to trace the distribution of illegal narcotics and synthetic substances such as pseudoephedrine and ephedrine.

The detection approach should use established techniques so that it can provide unambiguous responses.

The project will focus on employing multiple techniques, integrating them in a complex system in a complimentary approach, in order to identify an optimum trade-off between opposite requirements: compactness, simplicity, low cost vs. sensitivity, low false alarm rate, selectivity.

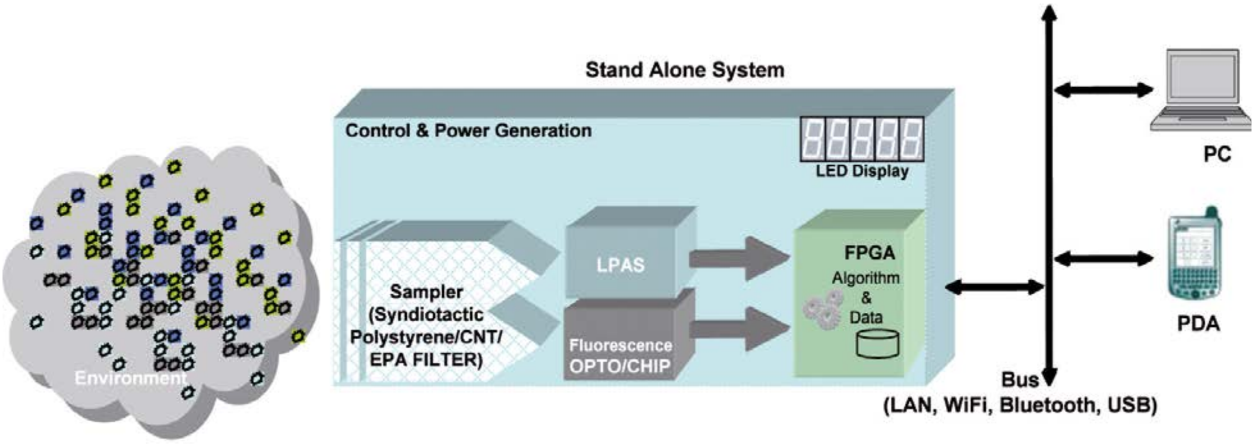
Description of the work

A drug precursor sensor demonstrator, implementing two main techniques will be developed:

- a low cost, high data throughput sensing technique, based on UV-Vis-NIR fluorescence which incorporates an array of different properly engineered chemical proteins able to bind the target analytes as happens in an 'immuno-type' reaction; and

- a highly sensitive and selective, compact and low weight, spectroscopic sensing technique in Mid-IR optical range, based on Laser Photo-Acoustic Spectroscopy (LPAS).

Parallel efforts will be spent on: identifying proper sampling techniques for both vapour and powder phase compounds; collecting or, where not existing, building up a database of characteristic spectra for both measurement techniques.


Stand Alone System
Control & Power Generation
LED Display
Environment
Sampler (Syndiotactic Polystyrene/CNT/ EPA FILTER)
LPAS
Fluorescence OPTO/CHIP
FPGA
Algorithm & Data
Bus
(LAN, WiFi, Bluetooth, USB)
PC
PDA

© Custom

Expected results

The sensor will be able to detect Drug Precursors such as ephedrine, P2P, BMK, Acetic anhydride and Phenylacetic acid and others compound with a screening time of 10 seconds.

PARTNERS	COUNTRY
SELEX Sistemi Integrati S.p.A.	Italy
GASERA	Finland
University of TURKU	Finland
INAS-Tecnalia	Spain
Alcatel-Thales III-V Lab	France
CNR IBP	Italy
ENEA	Italy
INSTM	Italy
Aalto University Foundation	Finland
Direction Nationale du Renseignement et des Enquêtes Douanières	France

DIRAC / Rapid screening and identification of illegal drugs by IR absorption spectroscopy and gas chromatography

© G.K. - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242309
Total Cost
€4,256,753.33
EU Contribution
€2,987,717
Starting Date
01/06/2010
End Date
31/03/2014

Coordinator

CONSORZIO CREO
CENTRO RICERCHE
ELETTRO-OTTICHE
SS 17 Localita Boschetto
L'Aquila 67100
Italy
Contact
Sandro Mengali
Tel: +39 0862346210
Fax: +39 0862346201
Website:
www.consorziocreo.it

Project objectives

The goal of this project was to develop an advanced sensor system that combines miniaturized Gas Chromatography (GC) as its key chemical separation tool, and Hollow-Fiber-based Infra Red Absorption Spectroscopy (HF-IRAS) as its key analytical tool to recognize and detect illicit drugs and precursors. Currently, GC-IRAS (through FTIR implementation) is, together with GC-Mass Spectrometry, the most powerful technique for the identification and quantification of amphetamines. However, so far it has been implemented only as bench-top instrumentation for forensic applications and bulk analysis. In DIRAC, the use of micromachined GC columns, solid state lasers, and hollow fibre IR, allow for developing a sensor that features hand-portability and prompt response –for field operation– and is able to perform both bulk and trace analysis. The DIRAC sensor further features a) an advanced sampling device, that separates the analyte from larger amounts of materials by electrostatic charging; and b), an advanced micro-machined pre-concentrator that treats sequentially both volatile ATS substances and non volatile ammonium salts.

Description of the work

The project was divided into into three phases as follows:

» Phase 1 (6 months), where requirements were reviewed;

» Phase 2 (24 months), where the sensor was developed together with its sensing modules, techniques and procedures;

» Phase 3 (12 months), where the sensor was tested, optimized and validated.

The main Work Package (WP) active in phase 1 was **WP1**, where a review was made of the target chemicals (amphetamines, precursors, and street compounds) and of the operational requirements for the sensor.

WPs active in phase 2 were :

» **WP2,** where the sensing prototype was developed, with its strategies, procedures, and process controls;

» **WP3,** that developed the sampling module, with its methods and procedures;

» **WP4,** that developed the pre-concentration module, with its methods and procedures;

» **WP5,** that developed the HF-IRAS module, with its methods and procedures;

» **WP6,** that developed the GC separation and detection module, with its methods and procedures;

» **WP7,** that developed the Expert System as a pattern recognition and learning machine.

The main WP active in phase 3 was **WP8**, where the sensor was tested and validated in the lab and through a small-scale field-campaign, and performance was assessed quantitatively, that was in terms of False Positive and False Negative Probabilities.

The Work-Plan further included a **WP0** (Management) and a **WP9** (dissemination and exploitation of results), both active throughout the project.

Results

The project developed three prototypes of diverse and complementary sensing capabilities:

- The first accepts liquid and solid traces on a swab, and recognises high specificity precursors and ATS free bases and salts, including street samples. Data is processed by an expert system (ES) that compares the measure with a reference database (DB), and additionally searches for similarities between unknowns and classes of psychoactive substances defined in the DB.
- The second analyses the air in search of volatile precursors. Since GC separation is here bypassed, response is faster, although less accurate.
- The third collects solid particles, precipitating those that, like ATS, have higher proton affinity, and uses surface ionisation to detect amine groups.

The three prototypes can, in principle, be combined into a unique sensor, by adding switching valves and fluidic bypasses.

A small scale demo was held by Customs at the Brussels National Airport. The sensors were successfully tested with negatives, precursors, and pre-precursors, including APAAN.

According to end users, the DIRAC sensor can fill a market gap by enabling reliable detection and identification of precursors, particularly in the case of 'big traces' and 'dirty' environment, where IMS sensors are prone to saturation and false alarms.

PARTNERS	COUNTRY
Consorzio CREO- Centro Ricerche Elettro-Ottiche	Italy
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Consiglio Nazionale delle Ricerche	Italy
EADS Deutschland GMBH	Germany
Selex Sistemi integrati SpA (SSI)	Italy
ELSAG DATAMAT S.p.A.	Italy
Universite de Lausanne	Switzerland
Universitatea Dunarea de Jos Din Galati	Romania
Institut National de Criminalistiek en Criminologie	Belgium
National Bureau of Investigation	Finland
Consorzio Interuniversitario Nazionale per la Scienza e la Tecnologia dei Materiali	Italy

EKSISTENZ / Harmonized framework allowing a sustainable and robust identity for European citizens

Information

Grant Agreement N°
607049
Total Cost
€6,753,638
EU Contribution
€3,482,175
Starting Date
01/06/2014
Duration
36 months

Coordinator

MORPHO (MPH)
Products and Innovation
11 Boulevard Gallieni
92445
92130 – Issy Les
Moulineaux – France
Contact
Stéphane Caillebotte
Tel: +33 1 58 11 34 26
Mobile: 33 6 43 85 49 45
Fax: +33 1 58 11 87 01
E-mail: stephane.caillebotte
@morpho.com
Website: www.morpho.com

Project objectives

The mission of EKSISTENZ is to deliver a comprehensive set of innovate and interoperable tools, procedures, methods and processes that will tackle identity theft in the EU.

The key objectives of EKSISTENZ are:

» Develop innovative and interoperable components that protect EU citizens from identity thieves;

» Assess the technical maturity of these tools by taking into account the outcome results of the proof of concept in a linked government/services environment;

» Strengthen citizen's privacy by generating trusted and dedicated secondary identity in a way that avoids function creep and crossing information between identities

» Provide member states with the option to implement these solution at national level;

» Inform EU citizens of the methods in place to recover her or his identity after theft;

» Detect identity fraud attempts and respond appropriately;

» Serve as a policy advisor to EU Member States;

» Build an identity theft think-tank community in cooperation with Interpol and Europol;

» Provide guidance to key actors via a European Observatory on identity theft..

Description of the work

EKSISTENZ will combat identity theft, typically committed via searching through recycled materials, phishing, spoofing, sending of scam emails or the targeted use of viruses, Trojans and key loggers. EKSISTENZ will do this by creating a real and strong link between the citizen and their primary identity document. It will:

» Strengthen the existing electronic-based primary identity document and associated bearer authentication method using biometric features and/or prior knowledge about the legitimate holder;

» Derive secondary identities of citizens from their primary identity document;

» Verify primary and secondary identities, and the bearers of such identities;

» Use the European network STORK in order to provide bilateral recognition solutions of primary identification between EU Member States.

Expected results

By achieving its objectives, EKSISTENZ will not only make a major contribution to the implementation of EU policy, but it will also open up the market for advanced identity protection systems – an international multi-billion Euro market – and will strengthen the position of Europe as a market leader in this domain.

In order to demonstrate the achievement of its mission, EKSISTENZ will develop a proof of concept relating to banking/finance that will be shown to be scalable and deployable at the national level.

PARTNERS	COUNTRY
Morpho (MPH)	France
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Eurosaft Sarl (IDP)	France
E-Forum Forum for European ePublic Services AISBL (EFO)	Belgium
Patrick Wajsbrot Consultants SAS (PWC)	France
Institute of Baltic Studies (IBS)	Estonia
Universidad Carlos III de Madrid (UC3M)	Spain
Katholieke Universitiet Leuven (KUL)	Belgium
DPA SIA (DPA)	Latvia
Bundesdruckerei GmbH (BDR)	Germany
Agenzia per l'Italia Digitale (AgID)	Italy
Ministry of the Interior of the Republic of Latvia (MIRL)	Latvia

HEMOLIA / Hybrid Enhanced Anti Money Laundering Intelligence, Investigation, Incrimination and Alerts

© brankatekic - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261710
Total Cost
€4,361,954
EU Contribution
€2,979,390
Starting Date
01/05/2011
End Date
30/04/2014

Coordinator

VERINT SYSTEMS LTD.
33 Maskit St Herzliya,
46733 Israel
Contact
Gideon Hazzani
Tel.: +972 9 9622596
Phone: +972 9 9622596
Fax: +972 9 962 4747
E-mail:
Gideon.Hazzani@verint.com
Website:
http://verint.com/corporate/

Project objectives

The overall mission of HEMOLIA is to research and develop an innovative anti-money laundering (AML) intelligent, multi-agent alert and investigation system.

Description of the work

The research to be performed in HEMOLIA can be divided into 3 categories:

1. Technological objectives: The technological research will be based on the envisaged HEMOLIA architecture composed of two main parts: (i) Data-collection and data-mining from the Financial Plane and from the Telecom Plane and (ii) the HEMOLIA Core Modules which will analyse the Telecom Plane and Financial Plane Data Sources and will create enhanced alerts.
2. Legal framework of AML Systems: The legal research will include several areas: Telecom Plane Legal Framework and the “Financial Plane Legal Framework” for different categories of end users (banks and financial institutes versusFIUs/LEAs). This will also include analysis of the content of alerts and harmonisation of AML-related data and boundaries.
3. AML end-users good practice and communication strategies including the definition of methodology and guidelines for an optimal use of the HEMOLIA system, information sharing methodologies between different authorities, at the national level and at the international level.

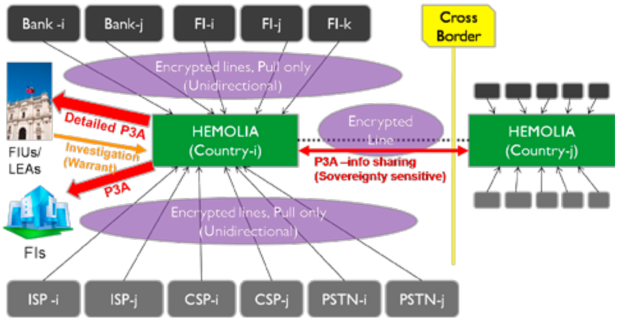
.

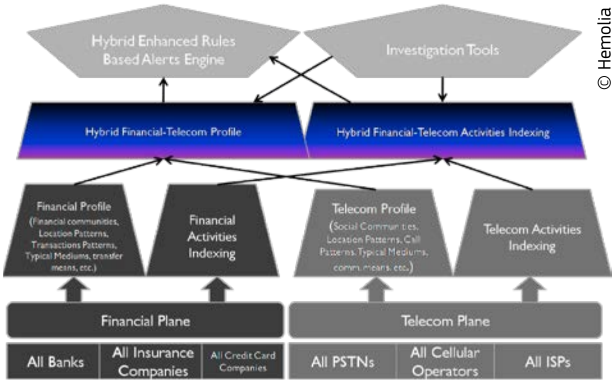
Results

The HEMOLIA functionalities support not only the internal processes of a FIU (Financial Investigation Unit) or LEA (Law Enforcement Agency), but also the relationship with the information providers. For instance, the system identifies cases of reporting where the information is not correct or complete and where it should be sent back to the reporting entity to be returned more accurate and value-added.

By using the alerting system, the end-user would be able to identify cases where the regulated entities should have provided the information. This will improve the relationship of the FIU with the reporting entities, by organizing more targeted training sessions and by providing more appropriate feedback.

© Hemolia




Hybrid Enhanced Rules Based Alerts Engine
Investigation Tools
Hybrid Financial-Telecom Profile
Hybrid Financial-Telecom Activities Indexing
Financial Profile (Financial communities, Location Patterns, Transactions Patterns, Typical Mediums, transfer means, etc.)
Financial Activities Indexing
Telecom Profile (Social Communities, Location Patterns, Call Patterns, Typical Mediums, comm. means, etc.)
Telecom Activities Indexing
Financial Plane
Telecom Plane
All Banks
All Insurance Companies
All Credit Card Companies
All PSTNs
All Cellular Operators
All ISPs

© Hemolia

PARTNERS	COUNTRY
Verint Systems Ltd.	Israel
MINISTRY OF JUSTICE	Denmark
OFICIUL NATIONAL DE PREVENIRE SI COMBATERE A SPALARII BANILOR	Romania
APLICACIONES EN INFORMATICA AVANZADA SA	Spain
CAPGEMINI NEDERLAND BV	The Netherlands
ZWIAZEK BANKOW POLSKICH IZBA GOSPODARCZA	Poland
UNIWERSYTET WROCLAWSKI	Poland
VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENTENZORG	The Netherlands
SWITCHLEGAL ADVOCATEN	The Netherlands
TELEKOMUNIKACJA POLSKA S.A.	Poland
Industrial Research Institute for Automation and Measurements PIAP	Poland
Ernst & Young	Israel

SAVEMED / Microstructure secured and self-verifying medicines

© SAVEMed

RESEARCH COMPLETED

Information

Grant Agreement N°
261715
Total Cost
€4,278,114.80
EU Contribution
€3,144,724.50
Starting Date
01/04/2011
End Date
31/03/2014

Coordinator

NANO-4-U GmbH
Mozartstrasse 7
D-76133 Karlsruhe
Germany
Contact
Stefan Klocke
Tel.: +49 (0) 721 182 69 68
Mobile:
+49 (0) 176 608 29 741
E-mail:
stefan.klocke@nano4u.net
Website: www.nano4u.net

Project objectives

Protecting EU citizens from counterfeit pharmaceuticals – SAVEmed offers comprehensive, user friendly and simple to implement solutions.

Counterfeit medicinal products are a threat to the health and safety of patients around the world. They range from drugs with no active ingredients to those with dangerous impurities.

They can be copies of branded drugs, generic drugs or over-the-counter drugs as well as faked implants or diagnostic devices.

In SAVEmed, self-verification security systems highly relevant for a secure track-and-trace system for the whole supply chain of a variety of medical products (e.g. solid dosage forms, pharmaceutical container, medical implants, and sterile pouches) will be developed. The key of the system is that it worked independent of external databases. It enabled the verification of the product's genuineness and its correct supply chain on-site at every step of this chain.

Description of the work

The project aim was to transfer diffractive gratings, random microstructures, micro-barcodes and contrast generating micro-prisms in hard tools. Moreover, algorithm enabling cross checking of the secure microstructures on the product (even through coatings) and on the package were developed to ensure the highest level of security possible. In SAVEmed, this direct product marking approach was realised for pharmaceutical tablets, injection moulded pharma caps and laminated sterile pouches.

Nevertheless the approach was applicable to nearly all other types of medical products.

The strategies of criminal organisations were analysed and the development was adapted to counteract these strategies. The key advantage of the implementation of secure microstructures directly in or on the medical product itself was that no chemical or biological additives and no costly changes of production lines were needed. Thus no additional approvals from regulatory agencies were required.

Results

The “Savemed” project successfully demonstrated the following:

1. A method of applying track & trace data to the drug itself (via a microstructure stamped onto the tablet surface during production), readable in <0.1s using a high-speed 3D scanner.

2. Self-verifying packages where the data on the tablets is scanned through the blister pack after packaging and verified against an ink-jet printed code on the reverse side of the pack.

3. Steel tooling inserts with integral holograms structured into the hardened steel surface that can be used to emboss holograms onto packaging or to make mould plastic parts with integral hologram structures without adding any extra materials or processes.

The hologram technology, integrated into a blister-packaging production line has been exhibited in Germany and the USA during 2015 in conjunction with a major pharmaceutical machinery manufacturer. The project co-ordinator, Nano4U GmbH, is discussing projects with several companies regarding further application of the steel hologram technology and of the tablet coding technology. Some of these companies are in the pharmaceutical field and others are in different industries. For example, a successful project was run during 2015 with a company to integrate a holographic security feature into steel tooling for a medical disposable device.

PARTNERS	COUNTRY
NANO4U GmbH	Germany
Heliotis AG	Switzerland
Centre Suisse d’Electronique et Microtechnique SA (CSEM)	Switzerland
SteriPack Ltd.	Ireland
Klocke Holding	Germany
Mauer Sp. z o. o,	Poland
United Nations Interregional Crime and Justice Research Institute (UNCRI)	Italy

SCIIMS / Strategic Crime and Immigration Information Management System

© khwi - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218223
Total Cost
€3,595,562.80
EU Contribution
€2,318,996.45
Starting Date
01/11/2009
End Date
31/10/2012

Coordinator

BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LIMITED
Commercial Department
Lyon Way, Frimley,
Camberley
GU16 7EX, Surrey
United Kingdom
Contact
Claire Dance
Tel: +44 (0)1276 603226
Mobile:
+44 (0)7793 423771
Fax: +44 (0)1276 603111
E-mail: claire.dance@baesystems.com
Website: http://www.sciims.co.uk/index.html

Project objectives

» Development and application of Information Management (IM) and Information Exploitation (IX) techniques enabling information to be fused and shared nationally and trans-nationally within a secure information infrastructure in accordance with European crime and immigration agencies' information needs;

» Development and application of tools to assist decision making in order to predict and analyse likely People Trafficking and People Smuggling sources, events and links to organised crime;

» Utilisation and enhancement of existing 'State of the Art' products to develop and incorporate new capabilities, 'Beyond State of the Art' into product baselines in order to speed up the introduction of new innovative techniques, technologies and systems.

Description of the work

People Trafficking and People Smuggling have long been a problem for European Governments, adversely affecting the security of their citizens. In many cases women and children are forced into the sex trade and subjected to labour exploitation. In formulating the SCIIMS project the consortium will focus upon an overarching research question from which the developed capabilities, demonstration and experiments will be focussed:

"In the European Union context how can new capabilities improve the ability to search, mine and fuse information from national, trans-national, private and other sources, to discover trends and patterns for increasing situational awareness and improving decision making, within a secure infrastructure to facilitate the combating of organised crime and in particular people trafficking/smuggling to enhance the security of citizens?"

The SCIIMS Consortium will utilise 'State of the Art' products which will form the base capability on which to develop new innovative capabilities and technologies. This approach is designed to provide an early exploitation opportunity for the consortium and the user groups involved.

Results

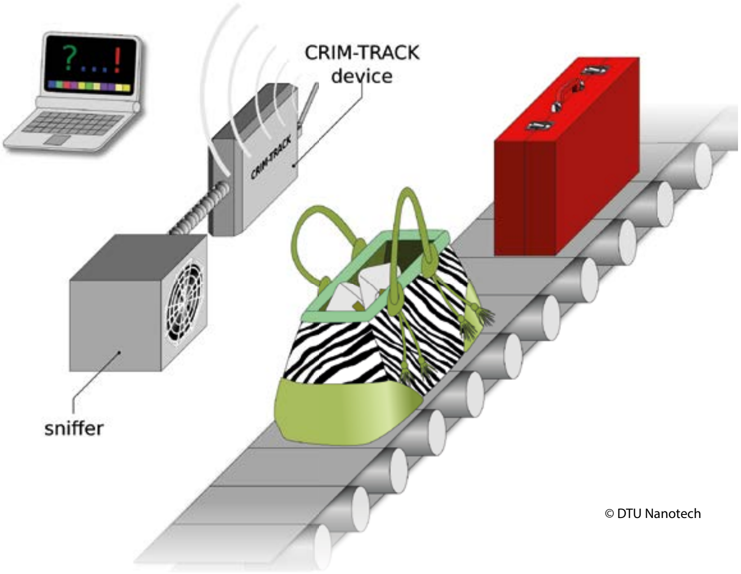
The project developed technology that collects information and fuses it to present a clearer picture of criminal activity and movements such as human trafficking.

The team focused on computer-based technology to strengthen the ability of LEAs to search, mine and fuse information from massive datasets obtained from diverse sources. Taking into account how investigators construct and represent data for an investigation, the research team produced an integrated demonstration system to show the effectiveness of their technologies, which support the various stages of an investigation, from the foraging for information to making sense of it.

According to the SCIIMS team, their project's technology could be very useful in detecting unusual and criminal behavior and preventing crime in Europe.

PARTNERS	COUNTRY
BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LTD	United Kingdom
INDRA SISTEMAS S.A. (INDRA)	Spain
COLUMBA GLOBAL SYSTEMS LTD (Columba)	Ireland
ELSAG DATAMAT S.P.A. (ED)	Italy
DENODO TECHNOLOGIES SL (DENODO)	Spain
Magyar Tudomanyos Akademia Szamitastechnikai Es Automatizalasi Kutato Intezet (Sztaki)	Hungary
UNIVERSIDADE DA CORUNA (UDC)	Spain
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
GREEN FUSION LIMITED (DATA FUSION)	Ireland

CRIM-TRACK / Sensor system for detection of criminal chemical substances



© DTU Nanotech

Information

Grant Agreement N°
313202
Total Cost
€4,844,602
EU Contribution
€3,583,940
Starting Date
01/01/2014
Duration
36 months

Coordinator

TECHNICAL UNIVERSITY OF DENMARK (DTU)
Department of Micro- and Nanotechnology
Ørsteds Plads 345
DK-2800 - Kgs. Lyngby - Denmark
Contact
Mogens Havsteen Jakobsen
Tel: +45 45255772
Mobile: +45 51801482
Fax: +45 45887762
E-mail: Mogens.Jakobsen@nanotech.dtu.dk
Website:
http://www.nanotech.dtu.dk/english
http://www.crimtrack.eu/

Project objectives

The detection of illegal compounds is an important analytical problem which requires reliable, selective and sensitive detection method that provides the highest level of confidence in the result. Moreover, to contribute to its successful development, automated target acquisition, identification and signal processing of data from the sensor are mandatory. Enhancements to sensing methods, recognition ability and timely target detection should improve sensors in both aspects, software and hardware. In the end, the sensing device should be portable, rapid, easy to use, highly sensitive, specific (minimal false positives), and low cost.

CRIM-TRACK - Sensor system for detection of criminal chemical substances aims to demonstrate a sensing device that can be further developed into a portable, miniaturized, automated, rapid, low cost, highly sensitive and simple, “sniffer”. This detection unit will be based on a disposable micro-colorimetric chip that can be used for identification of illegal drugs, drug precursors and home-made explosives.

The project will combine advanced disciplines such as organic chemistry, micro fabrication and hardware technology, machine learning and signal processing techniques to support the development of a miniaturized sensor system to identify illegal drugs or drug precursors. This will provide custom officers, police forces, etc. with an effective tool to control trafficking of illegal drugs and drug precursors.

Description of the work

» WP5 Micro-colorimetric chip for Sniffer system;

» WP7 Air sampling;

» WP8 Monitoring station;

» WP9 System integration;

» WP10 LEA Demo 1: Border control - Hidden drugs;

» WP11 LEA Demo 2: Checkpoint security - Hidden drugs;

» WP12 LEA Demo 3: Forensic investigation - Explosives.

Expected results

Development of Sniffer (prototype)

Road map for exploitation and protection of IPR

PARTNERS	COUNTRY
Technical University of Denmark (DTU)	Denmark
Cranfield University (CRA)	United Kingdom
Securetec GmbH (SEC)	Germany
Pro Design Electronic GmbH (PDE)	Germany
Gammadata Instruments AB (GIAB)	Sweden
Ministerie van Financien Directoraat Generaal Belastingdienst (DCA)	The Netherlands
Mykolas Romeris University (MRU)	Lithuania
Danish Emergency Management Agency (DEMA)	Denmark

LASIE / Large scale information exploitation of forensic data

Information

Grant Agreement N°
607480
Total Cost
€11,355,989.89
EU Contribution
€8,323,805.60
Starting Date
01/05/2014
Duration
42 months

Coordinator

ENGINEERING - INGEGNERIA INFORMATICA SPA (ENG)
Research and Development Division
Via San Martino Della Battaglia 56
00185 – ROMA - Italy
Contact
Maria Silvia BOI
Tel: +39 050 770342
Mobile: +39 3408100593
Fax: +39 0683074200
E-mail: silvia.boi@eng.it
Website: www.eng.it

Project objectives

The LASIE project aims to significantly increase the efficiency of current investigation practices, by providing an automated initial analysis of the vast amounts of heterogeneous forensic data that analysts have to cope with.

LASIE will:

» *automatically extract evidence* from different sources including video, audio, text, Internet, social networks, handwritten and calligraphic documents

» *perform inferences* based on the evidence

» *guide the investigation process* through the incorporation of recommendation functionalities

» *interact with the user* through an efficient and user-friendly interface

» *ensure that all legal and ethical restrictions are satisfied* and the computed data can be presented as evidence in European courts of law.

Description of the work

Amongst other challenges, LASIE will address the following tasks:

» Development of inference mechanisms taking into account analysts' explicit knowledge and information from previous cases

» Provision of an event-oriented module to link information from heterogeneous sources

» Implementation of an intuitive user interface that automatically highlights relevant events

» Implementation of training sessions to enable operators to use LASIE in an efficient manner

» Implementation of a privacy-by-design approach through built-in legal and ethical compliance mechanisms.

Expected results

Provision of a set of tools and processes to support law enforcement analysts in their everyday work.

Significant reduction of required investigation time by using automatic processes to analyze multimedia contents, as well as visual analytics from an inference engine that can highlight otherwise hidden information.

PARTNERS	COUNTRY
Engineering – Ingegneria Informatica SPA (ENG)	Italy
Centre for Research and Technology Hellas (CERTH)	Greece
Neuropublic A.E. Pliroforikis & Epikoinonion (NP)	Greece
Queen Mary and Westfield College, University of London (QMUL)	United Kingdom
Metropolitan Police Service (MET)	United Kingdom
SenseGraph Limited (SEN)	United Kingdom
Institutt for Fredsforskning Stiftelse (PRIO)	Norway
Huawei Technologies Duesseldorf GmbH (HUA)	Germany
Technische Universitat Berlin (TUB)	Germany
United Technologies Reasearch Centre Ireland, Limited (UTRCI)	Ireland
Innovation Engineering SRL (INNEN)	Italy
Venaka Media Limited (VML)	United Kingdom
ACIC SA (ACIC)	Belgium
Institut Mines-Telecom (IMT)	France
Universidad Politecnica de Madrid (UPM)	Spain
Visionware-Systemas de Informacao SA (VIS)	Portugal
Ayuntamiento de Madrid (ADM)	Spain
University of Greenwich (UoG)	United Kingdom

VALCRI / Visual Analytics for sense-making in CRIminal intelligence analysis

Information

Grant Agreement N°
608142
Total Cost
€16,644,340
EU Contribution
€13,053,686
Starting Date
01/05/2014
Duration
44 months

Coordinator

MIDDLESEX UNIVERSITY LONDON
The Burroughs, Hendon
London, NW4 4BT
United Kingdom
Contact
Professor B.L. William Wong
Tel: +44 (0)208 411 2684
Fax: +44 (0)208 411 6943
E-mail: w.wong@mdx.ac.uk
Website: valcri.org

Project objectives

The purpose of VALCRI (Visual Analytics for sense-making in CRIminal intelligence analysis) is to research, design and develop the next generation technology for information exploitation by intelligence analysts working in law enforcement agencies.

One of the key problems is to 'connect the dots' or to quickly find the relevant information from a very large dataset and piece them together so that the conclusion makes sense. When completed, VALCRI will integrate advanced and powerful data analytic software for automated extraction of meaningful information and related text, documents, images and video, and for detecting crime signatures or patterns across multi-dimensional data that might provide early warning signs or triggers of impending criminal or terrorist action.

Description of the work

VALCRI's analytical software capabilities will be orchestrated through a combination of commercially available and advanced touch user interface technologies. We will create new visual analytics interaction technologies for dynamically and directly manipulating the visualizations to facilitate the process of reasoning and analytic discourse as they computationally exploit large data sets and unravel the complexities in the data. VALCRI will augment rather than replace human judgment and decision making.

VALCRI will also design measures to guard against human cognitive bias and abuses arising from accidental, inadvertent, or deliberate violations of ethical, legal and privacy principles. The design of the technology will include facilities for ensuring transparency, openness, and accountability through information security, and safeguarding of privacy, bias mitigation, privacy by design, privacy enhancing technology, purpose limitation, and data minimisation.

The project is organised into 14 work packages that comprise: requirements; systems design and architecture; data extraction and analysis; data modeling and ontology; security, ethics, privacy and legal issues; user interface and cognitive issues; and training and evaluation.

Expected results

(i) A Human Issues Framework. The framework combines human cognition, bias mitigation, social, and legal factors into a single framework that developers can use to guide and specify the system design.

(ii) An interactive visualisation-based user interface. This advanced user interface is guided by the concept of the "reasoning workspace". The user interface will enable fluid and seamless transitions between data exploration, data analysis, and hypothesis formulation.

(iii) A real-time semantic search and retrieval engine that combines with automated knowledge extraction and thematic clustering. The system will allow users to develop interactive visualizations that help them explore the data at different levels of abstraction.

(iv) Automated knowledge extraction. VALCRI will develop automated methods for extracting relevant features to events from historical data. These features will be stored and updated regularly based on new incoming data to help define data fragments in real-time.

(v) A self-evolving ontology. The ontology will be informed by signature discovery, crime, and criminal profiling. It will also guide user search, retrieval, and navigation of data.

(vi) A crime situation re-construction function. This will be based on spatial-temporal and network analysis technologies for representing important socio-cultural and organizational concepts crucial for understanding the crime and circumstances, and to then project possible lines of investigation.

(vii) A secure and scalable distributed processing architecture. This architecture must be computationally efficient, able to accommodate high volume and high speed data from a variety of sources and content..

(viii) A research dataset. This will be machine readable, and based on real crimes that is of adequate size and complexity.

PARTNERS	COUNTRY
Middlesex University London	United Kingdom
Space Applications Services NV	Belgium
Universitat Konstanz	Germany
Linkopings Universitet	Sweden
The City University	United Kingdom
Katholieke Universiteit Leuven	Belgium
A E Solutions (BI) Limited	United Kingdom
Technische Universitaet Graz	Austria
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V.	Germany
Technische Universitaet Wien	Austria
ObjectSecurity Ltd	United Kingdom
Unabhaengiges Landeszentrum fuer Datenschutz	Germany
i-Intelligence GMBH	Switzerland
Exipple Studio SL	Spain
West Midlands Police Authority	United Kingdom
STAD ANTWERPEN	Belgium
Service Public Federal Interieur	Belgium

ZONeSEC / Towards a EU framework for the security of Widezones

Information

Grant Agreement N°
607292
Total Cost
€14,163,695.89
EU Contribution
€9,262,731.96
Starting Date
01/12/2014
Duration
48 months

Coordinator

EXODUS ANONYMOS ETAIREIA PLIROFORIKIS (EXO)
Exus Innovation
Estias 1 &
Mesogeion 73-75
11526 – Athens - Greece
Contact
Dr. Dimitris Kanakidis
Tel: +30 210 7450347
Mobile: +30 695 7211975
Fax: +30 210 7450399
E-mail: dkan@exus.co.uk
Website: www.exus.co.uk,
www.exusinnovation.co.uk

Project objectives

ZONeSEC aims to develop and integrate an innovative “Widezone” surveillance system.

» This will enable early detection and situational awareness assist authorities and operators regarding the prevention of illicit activities in even the most complex, remote or demanding localized spaces.

» Among its objectives is to improve the sensor base and sensor intelligence for high quality input for the system’s information fusion and processing framework in order to detect various kinds of illicit activity and patterns reduced rates of false alarms.

» The project aims to set a cornerstone for the standardization of equipment, network architecture, processes and methodologies for Widezones surveillance purposes on an EU level via pre-normative standards.

Description of the work

The ZONeSEC project suggests a multilayered digital security and surveillance system that will create a virtual perimeter (VP) around any Widezone facility. The system will be based on the use of acoustic fiber optics to detect any kind of intrusion inside the VP, plus ground and drone-based cameras (day and IR) and microwave sensors to further detect illicit pattern of activities. ZONeSEC will use expert reasoning, artificial intelligence and proprietary algorithms to simultaneously interpret scenes from multiple cameras and the data from the drones. All will be integrated into a user-friendly graphical user interface.

ZONeSEC will continuously monitor critical areas of industrial facilities, rail tracks, highways and water treatment facilities and other pervasive critical infrastructure. Finally, the project will pay careful attention to the total cost of ownership and operation of its solution with an eye to producing an efficient but economically viable system.

Expected results

ZONeSEC will create a robust and, more importantly, a scalable system to provide the same level of overview and situation awareness across all involved parties from different countries.

ZONeSEC expects to:

» Define a European-wide framework for the protection of Widezones, comprising a full-set of systems and services built according to innovative, integrated standards and peer-to-peer architecture, thus supporting illicit activity detection and early warning of emerging threats.

» Define a holistic data and information fusion architecture and develop beyond the state-of-the-art fusion technologies and algorithms to improve situation awareness and superior decision support.

» Deliver an advanced common operational picture via its state-of-the-art approach to the simulation and visualization of operations

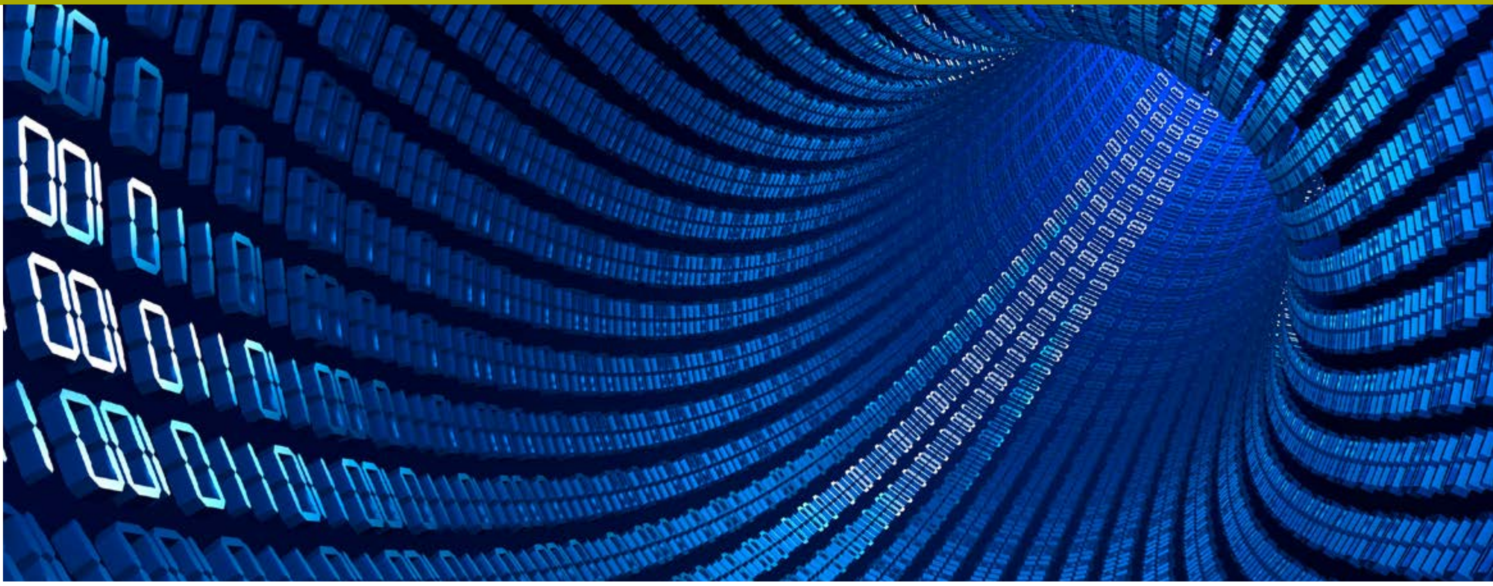
» Deliver detailed pilot demonstrations and integrity tests with an iterative approach that exploits end-user infrastructures such as:

- Water, gas and oil pipelines
- Railway networks
- Highways

- Contribute to the technical committees of the European Standardisation Organizations (ETSI and CENELEC) in conjunction with parallel workshop agreements and and an industrial specifications group.

PARTNERS	COUNTRY
Exodus Anonymos Etaireia Pliroforikis (EXO)	Greece
Diginext SARL (DXT)	France
Fundacion Tekniker (TEK)	Spain
Atos Spain SA (ATOS)	Spain
Technische Universität Dresden (TUD)	Germany
Istituto di Sociologia Internazionale di Gorizia (ISIG)	Italy
Airbus Defence and Space GmbH (AIRBUS)	Germany
University of Southampton (ITINNOV)	United Kingdom
Institute of Communication and Computer Systems (ICCS)	Greece
Crisisplan BV (CPLAN)	The Netherlands
Aditess Advanced Integrated Technology Solutions and Services Ltd (ADIT)	Cyprus
Gap Analysis S.A. (GAP)	Greece
Silixa Ltd (SIL)	United Kingdom
Thales Research and Technology (THALES)	France
Telesto Technologies Pliroforikis kai Epikoinonion EPE (TEL)	Greece
Attikes Diadromes S.A. (ATTD)	Greece
Compania AQUASERV S.A. (AQS)	Romania
N.V. Nederlandse Gasunie (GASU)	The Netherlands
Acciona Infraestructuras S.A (ACCI)	Spain

CAMINO / Comprehensive Approach to cyber roadMap coordINation and develOpment



Information

Grant Agreement N°
607406
Total Cost
€1,157,666
EU Contribution
€1,036,888
Starting Date
01/04/2014
Duration
24 months

Coordinator

ITTI SP. Z O.O. (ITTI)
ITTI Sp. z o.o.
Ul. Rubież 46
61-612 Poznań, Poland
Contact
Michal Choras
Tel: +48 61 6226 985
Fax: +48 61 6226 973
E-mail:
Michal.choras@itti.com.pl
Website: www.itti.com.pl

Project objectives

The major goal of the project is to provide a realistic roadmap for improving resilience against cyber crime and cyber terrorism. Its strategic objectives are to:

» develop a comprehensive cyber crime and cyber terrorism research agenda;

» initiate long term activities providing a stable platform of security research experts and organisations.

Description of the work

The main aim of the CAMINO project is to establish a research agenda on cyber crime and cyber terrorism in order to fully accomplish a trustworthy information society as depicted by the Digital Agenda 2020.

The work of the project is divided into the following activities:

» Project Management - WP1 will ensure the overall management of the project tasks in terms of effective completion, progress reporting, accountability and quality assurance. WP1 will be responsible for all contacts with the European Commission (deliverables delivery, reporting) and also with the project's advisory board, composed of external experts. A project handbook will be published that will guide the participants on administrative tasks and procedures for IPR, data handling, quality assurance, etc.

» Identification and Analysis of Main Research Gaps and Challenges - WP2 aims to identify key research gaps and challenges through analysis of existing cyber security-related guidelines, roadmaps and strategies. Promising results of current cyber security research projects will be identified and analysed.

» Workshops, Seminars and Consultations - WP3 will ensure the organisation of necessary activities and meetings for the consultation with experts, working groups and all involved stakeholders.

» Guidelines and Roadmap Development - WP4 will aim to develop cyber security guidelines, which will reflect the expectations and needs of key stakeholders. WP4 will identify key stakeholders and the scope of cyber security related problems. WP4 will also develop research roadmaps in the areas of cyber crime and cyber terrorism. This work is based on the activities of the other WPs. It will be based on commonly agreed needs among the stakeholders to provide effective guidelines and actions. Alignment with national initiatives is also planned.

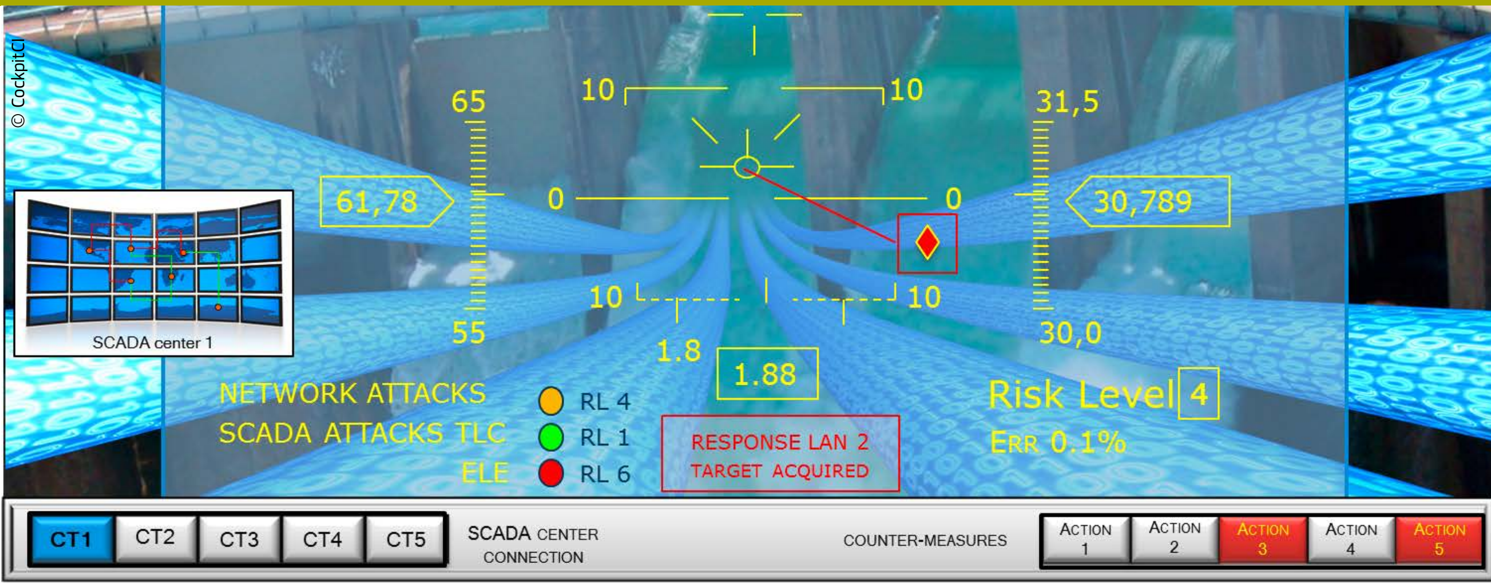
» Community Building, Dissemination and Sustainability - WP5 will provide analysis and determination of the most appropriate strategies for dissemination and exploitation of the project results and products.

Expected results

- the definition of a concept and terminology of cyber security, cyber crime and cyber terrorism;
- the identification of current cyber threats (including cyber crime and cyber terrorism) and corresponding state-of-the-art identification, protection and defence mechanisms, including appropriate risk analysis methodologies;
- the definition of research gaps and stakeholders needs;
- the guidelines, recommendations and a comprehensive research agenda (roadmap) regarding cyber security, cyber-crime and cyber terrorism;
- a long term cyber research community on the basis of the IMG-S Cyber Security Thematic Area (TA7).

PARTNERS	COUNTRY
ITTI Sp. z o.o. (ITTI) - Coordinator	Poland
CBRNE Ltd. (CBRNE Ltd)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR)	Italy
Data Fusion Research Center AG (DFRC)	Switzerland
Espion Ltd (Espion)	Ireland
Everis Aerospace and Defense S.L.U. (EADE)	Spain
Montpellier 1 University (UM1)	France
Police Academy in Szczytno (WSPol)	Poland
S21SEC Information Security Labs S.L. (S21SEC LAB)	Spain
Sec-Control Finland (Sec-Control Finland)	Finland

COCKPITCI / Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures



© CockpitCI

Information

Grant Agreement N°
285647
Total Cost
€4,234,558.35
EU Contribution
€2,986,675.00
Starting Date
01/01/2012
Duration
36 months

Coordinator

SELEX SISTEMI INTEGRATI SPA
Large Systems Business Unit
Via Tiburtina Km 12,400
00131 Rome, Italy
Contact
Antonio Graziano
Tel: +39 06 4150 2017
Mobile: +39 331 6231584
Fax: +39 06 4150 2356
E-mail:
agraziano@selex-si.com
Website: www.cockpitci.eu

Project objectives

CockpitCI aims to improve the resilience and dependability of Critical Infrastructures (CIs) by the automatic detection of cyber threats and the sharing of real-time information about attacks among CI owners.

CockpitCI aims to identify, in real time, the CI functionalities impacted by cyber-attacks and assess the degradation of CI delivered services.

CockpitCI aims to classify the associated risk level, broadcast an alert at different security levels and activate a strategy of containment of the possible consequences of cyber-attacks.

CockpitCI aims to leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety.

Description of the work

CockpitCI will design and develop a system capable of detecting malicious network traffic which may disrupt the correct functioning of a SCADA system and hamper its normal operability.

CockpitCI will rely on a unifying approach across the Critical Infrastructures modelling domain. Models and software tools will be used to predict the Quality of Services (QoS) delivered by SCADA systems early. Indicators of SCADA QoS will be computed using an adequate representation of the technological networks supporting SCADA services, including including multi-phased cyber attacks and accidental failures.

CockpitCI will aggregate the information of potential cyber-attacks induced on SCADA systems or telecommunication systems used to support the operation of CIs, and identify the potential unsecured area of the CIs.

CockpitCI will research traffic monitoring and attack detection. New machine learning based approaches for unusual traffic event detection will be analysed and several typologies of cyber-threats will be modelled, as will the cyber-interdependencies of the composite CIs system.

CockpitCI will provide a framework to allow the community of CI owners to exchange real-time information about attacks, extending the capabilities developed in the previous MICIE project. It will extend the prediction capabilities by considering cascading events induced by faults and cyber attacks and also develop a strategic analysis tool able to calculate the potential threat of coordinated cyber-attacks on CIs.

Expected results

The main expected result is the demonstration that the convergence among physical security, cyber security and business continuity is possible with positive fallouts for all the involved players. Benefits will arise from the security point of view thanks to the availability of a larger amount of field data, while, from the business point of view, a better real-time risk evaluation will allow a tailored definition of service level agreement and the avoidance of large domino effects.

PARTNERS	COUNTRY
SELEX Sistemi Integrati SpA (SELEX-SI)	Italy
Centre de Recherché Public Henri Tudor (CRPHT)	Luxembourg
Consortium for the Research in Automation and Telecommunication University of Rome - “La Sapienza” (CRAT)	Italy
Dipartimento Informatica e Automazione – Università di Roma Tre (ROMA3)	Italy
Agenzia nazionale per le nuove tecnologie, l’energia e lo sviluppo economico sostenibile (ENEA)	Italy
Israel Electric Corp (IEC)	Israel
itrust consulting s. à r. l. (ITRUST)	Luxembourg
Multitel asbl (Multitel)	Belgium
University of Coimbra Faculdade de Ciências e Tecnologia (UC)	Portugal
University of Surrey (SURREY)	United Kingdom

CRISALIS/ CRitical Infrastructure Security AnaLysIS

RESEARCH COMPLETED

Information

Grant Agreement N°
285477
Total Cost
€5,361,532.73
EU Contribution
€3,426,387.79
Starting Date
01/05/2012
End Date
31/08/2015

Coordinator

SIEMENS AG (SIE)
Corporate Technology RDA
ITS
Otto-Hahn-Ring 6
D-81730 Munich
Contact
Michael Munzert
Tel: +49 89 636 49603
Mobile: +49 173 7016288
Fax: +49 89 636 48000
E-mail: michael.munzert@siemens.com
Website:
www.crisalis-project.eu

Project objectives

O.1 Securing the systems

New techniques and tools to facilitate the automated analysis of critical infrastructure environments and the discovery of possible threat vectors.

O.2 Detecting intrusions

New techniques for the detection of targeted, unknown threats by avoiding a priori assumptions about attack-vector characteristics or those of malware samples.

O.3 Analyzing successful intrusions.

Methodologies for detecting suspicious modifications to devices, and forensic tools for the analysis of embedded devices typically used in these environments.

Description of the work

The CRISALIS project aimed to provide new means to secure critical infrastructure environments from targeted attacks carried out by resourceful and motivated individuals.

CRISALIS focused on two aspects: detection of vulnerabilities, and attacks in critical infrastructure environments. We focused on two different, yet interlinked, use cases typical to power grid infrastructure: control systems based on SCADA protocols and the Advanced Metering Infrastructure. CRISALIS leveraged the unique characteristics of critical infrastructure environments to produce novel practical mechanisms and techniques for their security assessment and protection. When addressing the project's three objectives particular attention was paid to ensure the practical implementation of these techniques in real-world environments. It also aimed to minimize the impact on operations, goals which are attainable thanks to the direct involvement of end users and device manufacturers who provided expertise and realistic test environments to validate the proposed methodologies.

Results

- » Build-up of four diverse test-beds and successful execution of 14 families of experiments
- » CRISALIS technologies from different work packages were combined to successfully detect and investigate a targeted attack
- » CRISALIS's passive ICS fingerprinting tool clearly outperforms existing (non-ICS specific) ones
- » Implementation of new protocol parsers for binary ICS protocols: Modbus/TCP, OPC-DA, and two proprietary protocols
- » CRISALIS developed a penetration testing methodology specifically tailored to critical infrastructures
- » CRISALIS's fuzzing tools helped identify and patch security vulnerabilities in several commercial products
- » The CRISALIS tool Avatar is the first one enabling sophisticated dynamic analysis on embedded devices

- ICS intrusion detection tool PLW proved to detect 0-day and targeted attacks (with low false positive rate on real-world traffic)
- CRISALIS's AMI intrusion detection prototype METIS proved able to detect complex attacks (e.g. energy exfiltration) with an accuracy of over 80 percent and low false positives, while being scalable to millions of devices
- The project's forensic platform FERRET reduced forensic investigation time in real-live incidents dramatically (by an order of magnitude)
- Its tool FCScan detected malicious electronic documents without prior knowledge
- CRISALIS's tools Grafiti and Access Miner detected malicious code at execution time and after a successful attack – again without prior knowledge

PARTNERS	COUNTRY
European Commission (EC)	Belgium
Siemens AG (SIE)	Germany
Alliander (ALL)	The Netherlands
Chalmers Tekniska Hoegskola (CHA)	Sweden
ENEL (ENEL)	Italy
Institute EURECOM (IEU)	France
SecurityMatters (SM)	The Netherlands
Symantec (SYMF)	France
University Twente (UT)	The Netherlands
University of Ulm (UULM)	Germany

COURAGE/ Cybercrime and Cyberterrorism European Research Agenda

RESEARCH **COMPLETED**

Information

Grant Agreement N°
607949
Total Cost
€1,681,477.60
EU Contribution
€1,294,425.50
Starting Date
01/05/2014
End Date
30/04/2016

Coordinator

EUROPEAN ORGANISATION FOR SECURITY (EOS)
Cybersecurity
Rue Montoyer
10
1000 – Brussels – Belgium
Contact
NINA OLESEN
Tel: +32 777 02 51
Mobile: +32 486 05 37 87
E-mail:
nina.olesen@eos-eu.com
Website: www.eos-eu.com

Project objectives

The aim of COURAGE is to produce a research agenda for Cybercrime and Cyberterrorism (CC/CT) using the expertise of the consortium partners, advisory board members and recruited expert stakeholders. The research agenda will identify the major challenges and reveal research gaps for cybercrime and cyberterrorism. It will also recommend practical research approaches to address these gaps through strategies that are aligned to real-world needs. These strategies will be supported by test and evaluation schemes. The purpose of COURAGE is to significantly improve the security of citizens and critical infrastructures and to support crime investigators.

Description of the work

A key challenge COURAGE will address is the speed of technological change. While the CC/CT regulatory, societal and technological research environment is constantly evolving, it remains dispersed across regions and institutions. There is currently no clear strategy on the best method to address the multi-disciplinary nature of CC/CT, and a lack of common terminology across disciplines hampers the adoption of a multidisciplinary approach. Research in CC/CT needs to focus on the development of concrete solutions with detailed tests and evaluation solutions, including complementary guidelines. COURAGE aims to solve this through its project approach, objectives and final roadmap.

The COURAGE approach builds on three pillars:

» A user-centric methodology - to identify gaps, challenges and barriers based on real-world needs and experiences

» An analytical and semantic approach - to deliver a taxonomy and create a common understanding of the subject with all stakeholders.

» A competitive and market oriented approach – to foster practical implementations of counter-measures using effective test and validation solutions.

The COURAGE research agenda will be elaborated through a progressive and collaborative approach, consolidating contributions from the legislative, law enforcement, research and industrial communities represented by its consortium and advisory board.

The agenda will be further supported by an online secure platform, fostering a collaborative approach during the elaboration phase offering a multi-lingual, advanced search interface. This will allow stakeholders to query the content of the agenda and acquire domain specific knowledge including statistical information about the most pertinent topics.

Expected results

The main results of COURAGE include:

- A taxonomical categorisation of CC/CT threats, supported by an online research knowledge repository, Community Portal, and mobile application
- An analysis of end-users requirements and of research gaps
- A final and validated research agenda, including roadmap and requirements for tests and evaluation
- The production of a consolidated roadmap in collaboration with the CAMINO and CyberROAD FP7 projects

PARTNERS	COUNTRY
European Organisation for Security (EOS)	Belgium
Engineering – Ingegneria Informatica SPA (EII)	Italy
Sheffield Hallam Unviersity (SHU)	United Kingdom
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Italy
Cybercrime Research Institute (CRI)	Germany
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Totalforsvarets Forskningsinstitut (FOI)	Sweden
West Yorkshire Police Authority (WYP)	United Kingdom
Aconite Internet Solutions Limited (ACO)	Ireland
Pawel Walentynowics (EEP)	Poland
Conceptivity SARL (CONC)	Switzerland
Institut Jozef Stefan (IJS)	Slovenia
Selex ES SPA (SSI)	Italy
Fraunhofer – Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FRAUN)	Germany
Stichting Katholieke Universiteit Brabant Universiteit Van Tilburg (TILT)	The Netherlands
International Cyber Investigation Training Academy Sdruzhenie (ICITA)	Bulgaria

ECOSSIAN/European Control System Security Incident Analysis Network

Information

Grant Agreement N°
607577
Total Cost
€13,196,720.61
EU Contribution
€9,224,459.00
Starting Date
01/06/2014
Duration
36 months

Coordinator

TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH (TEC)
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
Contact
Dr. Klaus-Michael Koch
Tel: +43 4242/ 233 55
Mobile: +49 173 7016288
Fax: +43 4242/ 233 55 77
E-mail: coordination@ecossian.eu
Website: www.ecossian.eu

Project objectives

ECOSSIAN's goal is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructure (CI) by implementing a pan-European early warning and situational awareness framework with command and control facilities. The project aims to develop a prototype system that facilitates preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management.

Description of the work

The protection of CI increasingly demands solutions that support incident detection and management for individual CI, across CIs that depend on each other, and across borders. An approach is needed that integrates functionalities across all these levels. Cooperation of privately operated CIs and public bodies (governments and EU) is difficult, but mandatory.

ECOSSIAN is the first attempt to develop such a holistic system. A prototype system will be developed to facilitate preventive functions such as threat monitoring, early indicator and real threat detection, alerting support of threat mitigation and disaster management. Advanced technologies need to be integrated with the technical architecture that comprises an operations centre and the interfaces of legacy systems (e.g. SCADA). Such technologies include fast data aggregation and fusion, visualization of the situation, planning and decision support, and flexible networks for information sharing and coordination support, as well as the connection of local operations centres.

Technical solutions will be complemented by an effective organizational concept and novel rules and regulations will be implemented. Also, the existing and required legal framework, information security and implications for privacy will be analyzed and assessed. The system will be tested, demonstrated and evaluated in realistic use cases to be developed with the community of stakeholders in the sectors of energy, transportation, finance, and ICT.

Expected results

» Establishment and enhancement of a security-state awareness to support CI operators by implementing an Operator Security Operation Centre (O-SOC)

» Combining identified O-SOCs of Member States' in a National Security Operation Centre (N-SOC)

» Improvement of the effectiveness of decision-making and incident response capabilities in Member States through near real-time situational awareness, information sharing and efficient command & control opportunities

» Support of a pan-European early-warning entity through the connection of Member States N-SOC to a European Security Operation Centre (E-SOC), including the required interoperability standards

» Enabling consistent and collaborative cross-border and cross-sectorial incident management for CI by using E-SOC and N-SOC capabilities

» Building trusted relationships and engage the CI operators at the EU level

- Ensuring trustworthiness, anonymity, privacy and legality of action for all stakeholders and end users as necessary

- Performance of a full-scale demonstration of the implemented ECOSSIAN framework and system

- Building an entry point for EU-US collaborative information sharing efforts in cyber defence to create readiness to react on a global basis.

PARTNERS	COUNTRY
Technikon Forschungs- und Planungsgesellschaft mbH (TEC)	Austria
Airbus Defence and Space GmbH (EADS)	Germany
Gas Networks Ireland (GAIS)	Ireland
Austrian Institute of Technology (AIT)	Austria
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung E.V. (FHG)	Germany
Alma Mater Studorium – Università di Bologna (UNIBO)	Italy
Cassidian Cybersecurity SAS (CAS-FR)	France
Inov Inesc Inovação – Instituto de Novas Tecnologias (INOV)	Portugal
Infraestruturas de Portugal SA (IP)	Portugal
Policia Judiciária (PJ)	Portugal
Espion Limited (ESPION)	Ireland
Teknologian Tutkimuskeskus (VTT)	Finland
Katholieke Universiteit Leuven (KUL)	Belgium
Bertin Technologies SAS (BRT)	France
Institut für Automation und Kommunikation e.V. Magdeburg (IFAK)	Germany
Poste Italiane (PI)	Italy
Cassidian Cybersecurity GmbH (CCG)	Germany
Cess GmbH Centre for European Security Strategies (CESS)	Germany
Airbus Group Ltd. (EADS UK)	United Kingdom

E-CRIME / The Economic Impacts of Cyber Crime

Information

Grant Agreement N°
607775
Total Cost
€3,749,289
EU Contribution
€3,004,180
Starting Date
01/04/2014
Duration
36 months

Coordinator

TRILATERAL RESEARCH & CONSULTING (TRI)
Crown House, 72 Hammersmith Road
W14 8TH, London, UK
Contact
Dr. Monica Lagazio
Tel: +44 207 559 3550
Mobile: +44 790 370 3051
E-mail: monica.lagazio@trilateralresearch.com
Website:
http://ecrime-project.eu

Project objectives

E-CRIME has two primary objectives:

1. Measure and analyse the economic impact of cyber crime on non-ICT sectors (e.g., transport, energy, finance, health etc) and analyse the criminal structures and economies behind such crimes.

2. Develop concrete measures and methods to deter possible criminals and to drastically limit the attractiveness of such crimes.

Description of the work

Progress has been made in understanding and managing cyber crime as well assessing its economic impact. Yet much remains to be done. Lack of co-ordination in law enforcement and legislation, lack of common consensus on the nature of cyber crime and lack of knowledge sharing and trust are just some of the issues that afflict cyber crime responses and cloud our understanding of cyber crime.

E-CRIME addresses these problems, while analysing the economic impact of cyber crime and developing concrete measures to manage risks and deter cyber criminals in non-ICT sectors. E-CRIME uses an interdisciplinary and multi-level-stakeholder focused approach that integrates a wide range of stakeholders' knowledge and insights into the project.

First, the project will develop a detailed taxonomy and inventory of cyber crime in non-ICT sectors and analyse cyber criminal structures and economies by combining the best existing data sources with specialist new insights from key stakeholders and experts.

Second, it will assess existing counter-measures against cyber crime in these sectors via current technology, best practices, policy and enforcement approaches, and awareness and trust initiatives.

Third, having mapped the as-is of cyber crime, the project will use available information and new data to develop a multi-level model to measure the economic impact of cyber crime on non ICT-sectors.

Fourth, it will integrate all the findings to identify and develop diverse, concrete counter-measures, combined in portfolios of inter-sector and intra-sector solutions, including enhancement for crime-proofed applications, risk management tools, policy and best practices, and trust and confidence measures.

Expected results

E-CRIME’s work aims for thefollowing durable impacts:

1. Increasing awareness of policy makers

2. Helping businesses to provide crime-proofed applications

3. Increasing the trust and confidence of EU citizens in using cyber applications

4. Making the European Union’s security work programme more effective

PARTNERS	COUNTRY
Trilateral Research & Consulting (TRI)	United Kingdom
Technische Universiteit Delft (TUD)	The Netherlands
Universite De Lausanne (UNIL)	Switzerland
Westfaelische Wilhelms-Universitaet Muenster (WWU)	Germany
The University of Warwick (WARWICK)	United Kingdom
Rijksuniversiteit Groningen (RUG)	The Netherlands
Global Cyber Security Center (GCSEC)	Italy
IPSOS Belgium SA (IPSOS)	Belgium
Tallinna Tehnikaulikool (TUT)	Estonia
The International Criminal Police Organisation (INT)	France

HYRIM / Hybrid Risk Management for Utility Networks

Information

Grant Agreement N°
608090
Total Cost
€4,657,587.60
EU Contribution
€3,387,085.00
Starting Date
01/04/2014
Duration
36 mois

Coordinator

AIT – AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)
Safety & Security Department
Donaucitystrasse 1
1220 Vienna, Austria
Contact
Monyk Christian
Tel: +43 50550 4152
Mobile: +43 664 8157837
Fax: +43 50550 4190
E-mail:
christian.monyk@ait.ac.at
Website: www.ait.ac.at

Project objectives

The main objective of this project is to identify and evaluate “hybrid risk metrics” for assessing and categorizing security risks in interconnected utility infrastructure networks in order to provide the basis for new protection and prevention mechanisms.

HyRiM will look at attacks that specifically target utility network controls as well as novel threats along interconnected utility networks. It will investigate the “human factor” and the impact of organizational aspects on security, the use of personally owned communication devices and the application of “on demand” surveillance to secure the extended perimeter.

Description of the work

During the project we will focus on sensitive service parameters that represent interconnection points between control networks and individual utility networks since, through them, a security incident in the control network could lead to cascading effects in utility networks. Hence we refer to our approach as “Hybrid Risk Management” and “Hybrid Risk Metrics”.

The risk measures to be developed will support a quantitative risk analysis and simulation tools for decision makers and security specialists as they evaluate threats. To unify the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis, our framework will support a qualitative assessment with a sound quantitative mathematical underpinning.

Furthermore we consider “the human factor” in our investigations. As a result of this, all the sociological and economic effects across different networks will be well understood. We will evaluate identified security measures and hybrid risk metrics in use cases involving various attack scenarios on the control network. Special attention will be paid to scenarios in which personally owned communication devices used in business day to day life compromise the security of a utility control network.

Another core topic of interest is the combination of monitoring and surveillance of the extended perimeter by triggering “on demand” surveillance by monitoring events to provide the basis for novel surveillance mechanisms.

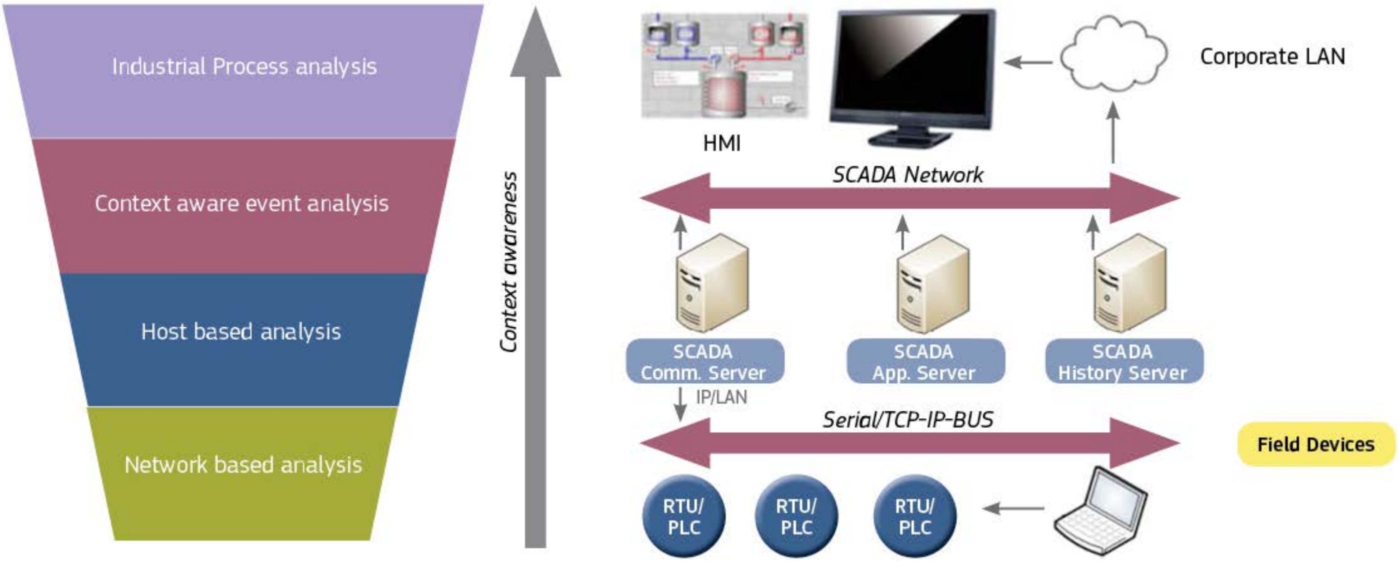
Expected Results

The project will provide utility network providers with a risk assessment tool that – in accordance with BSI or ICNC recommendations – supports qualitative risk assessment based on numerical (quantitative) techniques. Our research method will explicitly account for an infrastructure's two-fold nature in terms of the utility network and the control network alongside it.

The expected impact is thus a movement away from best-practice-only towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

PARTNERS	COUNTRY
(P2) Universität Passau (UNI PASSAU)	Germany
(P3) Lancaster University (ULANC)	United Kingdom
(P4) ETRA Investigacion y Desarrollo SA (ETRA)	Spain
(P5) Akhela SRL (AKH)	Italy
(P6) Suministros Especiales Alginetenses Coop.V. (ECA)	Spain
(P7) Linz AG für Energie, Telekommunikation, Verkehr und Kommunale Dienste (LINZ AG)	Austria

PREEMPTIVE / Preventive Methodology and Tools to Protect Utilities



Information

Grant Agreement N°
607093
Total Cost
€5,204,569.68
EU Contribution
€3,831,016.24
Starting Date
01/03/2014
Duration
36 months

Coordinator

VITROCISET S.P.A. (VITRO)
Giorgio Sinibaldi
Via Tiburtina, 1020
00156 – Rome – Italy
Contact
Giorgio Sinibaldi
Tel: +39 068820 4394
Mobile: +39 3346196030
Fax: +39 068820 4269
E-mail: g.sinibaldi@vitrociset.it
Website: www.vitrociset.com

Project objectives

PREEMPTIVE's goal is to provide an innovative solution against cyber attacks that target utility networks by enhancing existing methods and conceiving new tools. PREEMPTIVE addresses the prevention of cyber attacks against hardware and software systems such as DCS, SCADA, PLC, networked electronic sensing, and monitoring and diagnostic systems used by the utilities networks. Moreover, the research aims to implement detection tools based on a dual approach comprised of low direct detection and process misbehavior detection.

PREEMPTIVE proposes to enhance existing methodological security and prevention frameworks with the aim of harmonizing Risk and Vulnerability Assessment methods, standard policies, procedures, and applicable regulations or recommendations to prevent cyber attacks. Its dual approach takes into account both the industrial process misbehavior analysis (physical domain) and the communication & software anomalies (cyber domain).

Description of the work

PREEMPTIVE proposes to face the new threats trends against SCADA and industrial networks, using jointly a methodology framework and innovative techniques; both will be strongly related in order to fill the existing gaps among security policy, practices and technologies. The heavy involvement of the utility companies partnered within the consortium assures the feasibility of this goal.

A specific "host based" technique will be developed in order to contrast transmission through personal devices. The impact of the "host based" tool envisaged will also be within the sector of the "cloud technologies" especially for securing storage spaces.

PREEMPTIVE enhances existing security frameworks with the aim of harmonizing Risk and Vulnerability Assessment methods, standard policies and procedures and applicable regulations or recommendations. In details ISO/IEC 27000 family of standards will be considered as well as the outcomes coming from other FP7 projects: NI2S3, MICIE and COCKPITCI dealing with Cyber Security and Critical Infrastructure protection.

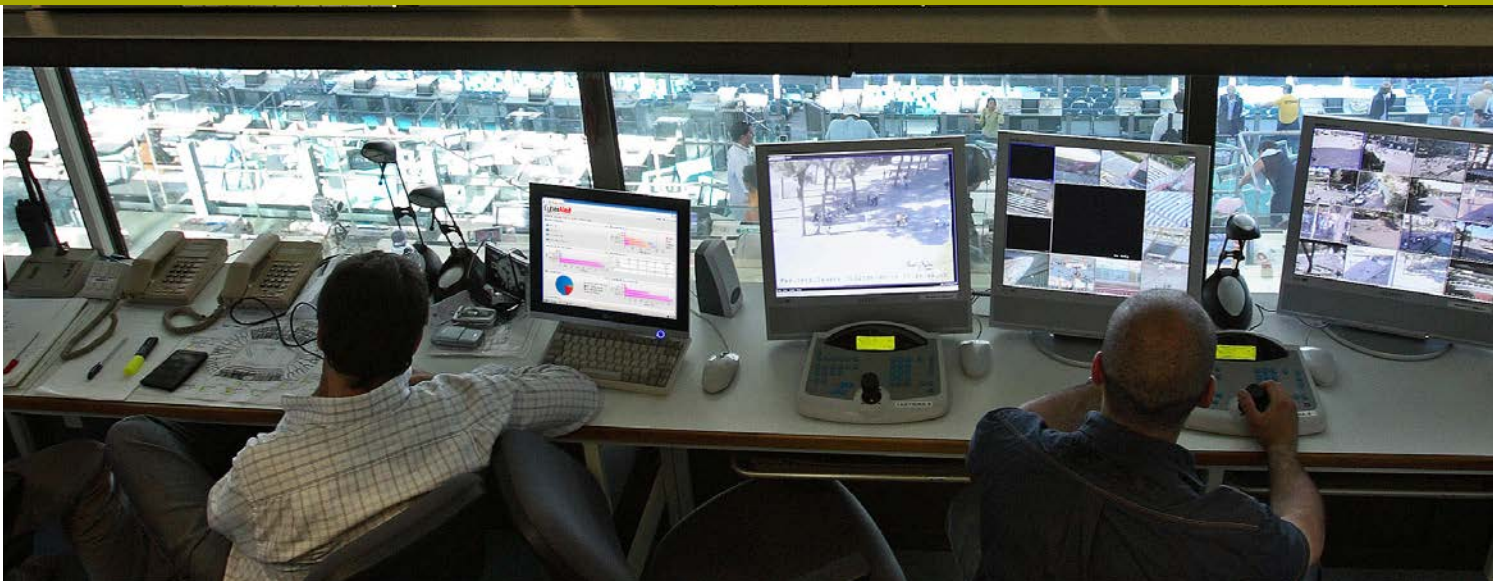
Expected results

We expect to have a high impact on utility companies and related industry and it is highly likely that future attacks will be thwarted with the help of PREEMPTIVE project results.

The outcomes envisaged in PREEMPTIVE shall improve the awareness in legal and regulatory organizations as well as for operators managing critical infrastructure assets.

PARTNERS	COUNTRY
Vitrociset SpA (Vitro)	Italy
Universiteit Twente (UT)	The Netherlands
SecurityMatters BV (SM)	The Netherlands
Aplicaciones en Informática Avanzada S.L. (AIA)	Spain
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (IOSB)	Germany
HW Communication Limited (HWC)	United Kingdom
Università degli studi Roma Tre (UNIROMA)	Italy
European Network for Cyber Security U.A. (ENCS)	The Netherlands
Israel Electric Corporation Limited (IEC)	Israel
Katholieke Universiteit Leuven (KU Leuven)	Belgium
Fundacio Institut de Recerca de l’energia de Catalunya (IREC)	Spain
Harnser Ltd (HARNSER)	United Kingdom

SAWSOC / Situation AWare Security Operations Center



Information

Grant Agreement N°
313034
Total Cost
€5,406,398.00
EU Contribution
€3,491,379.00
Starting Date
01/11/2013
Duration
30 months

Coordinator

SELEX ES SPA (SELEX ES)
Cyber Security & Information Assurance
Via Tiburtina Km 12 400
00131 – Roma - Italy
Contact
Giuseppe La Posta
Tel: +39 06 5027 4742
E-mail: Giuseppe.laposta@selex-es.com
Website:
www.selex-es.com
www.sawsoc.eu/

Project objectives

The objective of SAWSOC is to identify, implement, and validate techniques to achieve the convergence of physical and logical solutions for security monitoring. This entails the following:

1. Advancing and modernising some of the key physical and logical security technologies (namely: SOC, SIEM, Video Surveillance, PSIM, IM, Forensics, and Building Automation)

2. Developing techniques for correlating physical and logical security services from the physical and electronic domains to achieve a consistent view and to be able to produce an irrefutable record of who did what, where, and when

3. Implementing those techniques in an integrated platform for providing sophisticated security services combining in modular way diverse information from multiple sources

Description of the work

SAWSOC aims to effect a significant advancement in the convergence of physical and logical security, meaning effective cooperation among previously disjointed functions. The project is implemented in 3 main steps.

The first phase, basically consisting in detailed definition/planning of project objectives and activities, started in November 2013 and ended in late April 2014. As an important milestone, the requirements have been identified and the techniques which will have to be implemented by the SAWSOC components and platform have been defined. Second, the project will focus on the prototype implementation until mid-2015. Then, a first workshop will then be organized, to present preliminary results to a wider audience, and collect feedback. The final workshop will take place at the end of the project in 2016.

Expected results

Demonstrating and validating the proposed techniques and the framework by performing a thorough experimental campaign with respect to three substantial case studies, namely: “maintenance impacts and attack recognition on critical infrastructures” (MIARCI); “energy production and distribution critical infrastructure” (EPDCI); and “crowded events safety & security” (CES&S).

In addition to experimental evaluation in the domains of the three use cases, the consortium will study the applicability of the proposed solutions to a wider scope, i.e. to critical infrastructure domains other than air traffic management and energy production, and to crowded events in contexts other than sports.

Experiments will also be used to derive best practices for optimal deployment of the security technologies in real world settings.

PARTNERS	COUNTRY
Selex ES (SELEX)	Italy
Consorzio Interuniversitario Nazionale per l’Informatica (CINI)	Italy
Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FhG-IOSB)	Germany
The Israel Electric Corporation Limited (IEC)	Israel
Enav SPA (ENAV)	Italy
Intercede Limited (INTRCED)	United Kingdom
Espion Limited (ESPION)	Ireland
Lonix Oy (LONIX)	Finland
Bergische Universitaet Wuppertal (BUW)	Germany
Esaprojekt SP Z OO (ESA)	Poland
Comarch S.A. (CMR)	Poland

SECCRIT / Secure Cloud Computing for Critical Infrastructure IT

© Thinkstock

Information

Grant Agreement N°
312758
Total Cost
€4,802,313
EU Contribution
€3,397,319
Starting Date
01/01/2013
Duration
36 months

Coordinator

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)
Safety & Security Department
Donau-City-Straße 1
1220 Vienna
Contact
Thomas Bleier (Thematic Coordinator ICT Security)
Tel: +43 664 8251279
Fax: +43 50550 2813
E-mail:
thomas.bleier@ait.ac.at
Markus Tauber (Project Manager SECCRIT)
Tel: +43 664 8251011
Fax: +43 50550 2813
E-mail:
markus.tauber@ait.ac.at
Website: www.seccrit.eu

Project objectives

The SECCRIT project is a multidisciplinary research project with the mission to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments. It will develop methodologies, technologies and best practices for creating a secure, trustworthy and high assurance cloud computing environment for critical infrastructure IT.

Description of the work

Cloud computing is a style of computing where elastic IT-related capabilities are provided as optimized, cost-effective, and on-demand utility-like services to customers using Internet technologies. Being one of the major trends in the IT industry recently, it has gained tremendous momentum and started to revolutionize the way enterprises create and deliver IT solutions.

As more sectors adopt cloud services in their computing environment, the trend will also reach ICT services operating critical infrastructures (CI), such as transportation systems or infrastructure surveillance. Hosting CI services in the cloud brings with it security and resilience requirements that existing cloud offerings are not well placed to address.

Due to the opacity and elasticity of cloud environments, the risks of deploying CI services in the cloud are difficult to assess – specifically on the technical level, but also from legal or business perspectives. Traditional IT security measures cannot fully tackle the issues (e.g. risk, trust, and resilience) arising from this paradigm shift, especially for operators and manufacturers of CI IT systems.

Therefore, the mission of the SECCRIT project is to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for CI.

To accomplish this, the objectives of the SECCRIT project are:

» identification of the relevant legal framework and establishment of respective guidelines, provision of evidence and data protection for cloud services;

» understanding and managing risk associated with cloud environments;

» understanding cloud behaviour in the face of challenges;

» establishment of best practice for secure cloud service implementations;

» demonstration of SECCRIT research and development results in real-world application scenarios

Expected results

- » Establishment of legal fundamentals by identification and techno-legal modelling of legally subsumable scenarios
- » Methodologies and tools for risk assessment, policy specification and enforcement and assurance evaluation
- » Techniques for cloud analysis and forensics, frameworks for resilience management
- » Process-oriented security guidelines for critical infrastructure cloud services
- » Evaluation and application of SECCRIT results in two real-world pilot scenarios dealing with hosting of video surveillance and critical mobility services

PARTNERS	COUNTRY
AIT Austrian Institute of Technology GmbH (AIT)	Austria
ETRA Investigacion y Desarrollo, S.A. (ETRA)	Spain
Fraunhofer IESE (IESE)	Germany
Karlsruhe Institute of Technology (KIT)	Germany
NEC Europe Ltd. (NEC)	United Kingdom
Lancaster University (LANC)	United Kingdom
Mirasys Ltd. (MIRASYS)	Finland
Hellenic Telecommunications Organization S.A. (OTE)	Greece
Ajuntament De Valencia (VALENCIA)	Spain
Amaris (AMARIS)	Austria

DESURBS / Designing safer urban spaces

© Bezalel Academy

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261652
Total Cost
€4,161,929
EU Contribution
€3,208,549
Starting Date
31/12/2014
End Date
48 months

Coordinator

RESEARCH MANAGEMENT AS
Fortunalia 14
NO-7057 Jonsvatnet,
Norway
Contact
James Rydock
Tel: +47 73919307
Mobile: +47 95907562
Fax: +47 73918200
E-mail: jrydock@researchmgt.com
Website: www.desurbs.net

Project objectives

» Establish a security events database with a representative number of incidents resulting from security threats in urban areas;

» Create an Integrated Security and Resilience (ISR) design framework that engages local stakeholders in a local forum for finding weak points and strengthening urban spaces;

» Develop GIS-based mapping and visualization tools based on urban design case studies;

» Develop comprehensive supporting models, technologies and tools for quantifying vulnerabilities and strengthening weaknesses;

» Develop and implement a Decision Support System Portal integrating the database, the ISR framework, the mapping and visualization tools and the comprehensive supporting models, technologies and tools;

» Develop an objective rating scale for quantifying safety of different urban space designs and use it to show that the DESURBS solutions result in urban spaces less prone to and less affected by security threats;

» Carry out case studies in Jerusalem, Barcelona and Nottingham.

Description of the work

The project was divided into seven work packages (WPs). WP1 established an urban security and resilience database that looked at a range of past urban security incidents and 'near misses'. The database informed the identification of weak points in a variety of urban spaces in cities old and new, as well as the design of more robust and resilient urban spaces. As part of this development, we created an objective scale for quantifying the safety and security of different urban space typologies and designs. This was a key feature for showing that DESURBS designed result in urban spaces that were less prone to and less affected by security threats.

WP2 elaborated an Integrated Security and Resilience (ISR) design assessment framework. This was a multidisciplinary methodology that engaged local stakeholders and focus groups to help recognize and understand the risks and vulnerabilities present, in the context of the competing functionalities (social, economic, aesthetic, managerial) and limitations in a given urban area. WP3 developed mapping and visualization tools to facilitate efficient use of the project's outputs. WP4 developed and adapted supporting models, tools and technologies that advance the state-of-the-art for quantifying different vulnerability aspects of urban spaces to identified threats and risks, to be used to help carry out the ISR design methodology within the framework developed in WP2. The WP2, WP3 and WP4 activities were informed and developed with reference to case studies in Jerusalem, Barcelona and Nottingham, where the project has established ties with local governmental and municipal planning authorities. WP5 combined all of the above into an internet-based, user friendly Decision Support System Portal. WP6 and WP7 were for dissemination and management, respectively.

Results

DESURBS results include new methodologies, various databases and software tools. The latter may be used either singly or in combination with the project's decision-support system portal (DSSP). This easy-to-use Internet based portal is targeted at urban planners, designers and engineers.

The DSSP helps stakeholders to recognise and rectify security weaknesses in urban designs, based on current best practices. Certain databases estimate the strengths of common building materials, while others provide tools for assessing weak points in buildings. The package also includes a modelling tool for simulating urban catastrophe management scenarios.

Further outcomes involved development and testing of mobile phone applications for crowd monitoring and tracking and for citizens' communications with authorities. The project also devised a tethered balloon system to facilitate emergency communication. The DESURBS toolset helps authorities plan for and manage urban disasters, including natural and human-caused. The result means an improvement in safety for urban residents and better emergency response.

PARTNERS	COUNTRY
Research Management AS (Resman)	Norway
Loughborough University (Loughborough)	United Kingdom
The University of Birmingham (Birmingham)	United Kingdom
The Hebrew University of Jerusalem (HUJI)	Israel
Technical University of Crete (TUC)	Greece
Centre Internacional de Metodes Numerics en Enginyeria (CIMNE)	Spain
University of Southampton (IT Innovation)	United Kingdom
Bezalel, Academy of Arts and Design (Bezalel Academy)	Israel

ELASSTIC / Enhanced Large scale Architecture with Safety and Security Technologies and special Information Capabilities

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312632
Total Cost
€5,286,041.00
EU Contribution
€3,472,071.00
Starting Date
01/05/2013
End Date
30/04/2016

Coordinator

NETHERLANDS ORGANISATION FOR APPLIED SCIENTIFIC RESEARCH (TNO)
Explosions Ballistics and Protection
Schoemakerstraat 97
PO Box 6060
2600 JA Delft,
The Netherlands
Contact
Mrs. Ans van Doormaal
Tel: +31 8886 61294
Mobile: +31 6 11783040
E-mail:
Ans.vandoormaal@tno.nl
Website: www.tno.nl

Project objectives

ELASSTIC's objective was to improve the security and resilience of large scale multifunctional building complexes to natural and man-made disasters by providing a methodology and tools which enable to include security and resilience from the early design and planning phase of such projects.

Description of the work

The ELASSTIC concept was based upon the following key features:

1. A comprehensive approach for designing safe, secure and resilient large scale building infrastructures
2. A set of tools to enable architects, structural engineers and building installation engineers to assess the safety, security and resilience of designs and to optimise the integral design
3. Coupling and integration of these tools into State of the Art Building Information Modelling (BIM) technology resulting in Extended BIM technology (BIM+)
4. Smart and reinforced building elements to measure the actual building condition combined with an increased bearing capacity and resistance
5. Coupling and integration of BIM and BMS (Building Management System)
6. Real time information on the safety, security and resilience of infrastructure

Results

Validation (Proof of Concept) of the approach and developed tools were done by evaluating the design of a multifunctional, resilient, large scale urban complex (anno 2020), called the ELASSTIC complex. This fictitious complex was designed in the project. This large multifunctional complex combined housing, shopping centre, transport node, business centre and entertainment centre. In this design, safety and security were integrated to make the complex resilient to natural and manmade threats.

The ELASSTIC complex was not only secure and resilient to disasters, it was also designed to ensure fast and efficient evacuation in case of a disaster. For a crowded complex comprising a large number of people, the design of a smart evacuation system should be included at the start of the complex design. Taking evacuation and safety installations into account in the design phase increased safety and was less expensive compared to an evacuation system integrated after the complex was build or at the final design stage.

PARTNERS	COUNTRY
Nederlandse organisatie voor toegepast natuurwetenschappelijk onderzoek – TNO (TNO)	The Netherlands
Fraunhofer-geselschaft zur foerderingen der Angewandten Forschung - Ernst Mach Institute (EMI)	Germany
Schüßler-Plan Ingenieurgesellschaft GmbH (SP)	Germany
Siemens AG (SIE)	Germany
Arcadis Nederland B.V. (ARC)	The Netherlands
Instituto Consultivo para el Desarrollo – Incode (INCODE)	Spain
North by Northwest Architectures – NXNW (NXN)	France
Uniresearch B.V. (UNR)	The Netherlands
Joubert Architects (JA)	The Netherlands

HARMONISE / Holistic Approach to Resilience and Systematic Actions to make Large Scale UrbaN Built Infrastructure Secure

Information

Grant Agreement N°
312013
Total Cost
€4,144,140.52
EU Contribution
€3,493,771.00
Starting Date
01/06/2013
Duration
36 months

Coordinator

FUTURE ANALYTICS CONSULTING LTD (FAC)
23 Fitzwilliam Square (South)
Dublin 2, Ireland
Contact
Dr. William Hynes
Tel: +353 (0) 1 639 4836
Mobile:
+353 (0) 86 852 4438
Fax: +353 (0) 1 554 7334
E-mail: william.hynes@futureanalytics.ie
Website:
http://futureanalytics.ie/

Project objectives

The HARMONISE project will assess the vulnerability of urban infrastructure and will forge new opportunities for enhancing resilience of large scale urban built infrastructure. The concept will be designed for use by civil authorities/municipalities and other key stakeholders involved in the design, planning, construction, operation or use of large scale urban built infrastructure.

Specifically, HARMONISE will:

- Deliver supporting tools (hosted within the platform) for the design/planning stage of large scale urban built infrastructure development; these will be tested/enhanced through quality case studies;

- Provide an integrated approach to sharing building infrastructure and security information including critical flows of materials/energy and sensor technologies etc., while recognising the important role of security culture and societal acceptance aspects;

- Be conducive to complementarities with other EU FP7projects, not least VITRUV, BESECURE, RIBS and DESURBS;

- Advocate and promote a significant exploitation programme to capitalise on new market opportunities, thus enhancing the pool of European expertise supported by a comprehensive education/training curriculum; and, ultimately,

- Improve the design of urban areas and systems by increasing their security against, and resilience to, new threats.

Description of the work

The project will culminate in a holistic concept of innovative technology exploitation. This will be achieved by the development of a versatile, intuitive and interactive intelligence platform, with semantic data processing capabilities. Within this,all aspects of urban security and resilience are enshrined.

Developing a practical and holistic concept which addresses the range of complexities inherent in urban resilience, while fulfilling the objective of enhanced resilience in a sustainable way (and also ensuring acceptability by citizens).

HARMONISE will be a milestone project in the field of resilience, making a major contribution toward minimising the destruction and lethality arising from a range of potential disasters. It will provide solutions for adapting and responding to disaster scenarios, while also integrating aspects for the long term sustainability of large scale urban built infrastructure such as energy efficiency and multi-functionality.

Expected results

The final validated version of the HARMONISE platform is an interactive, holistic approach providing versatile support for end-users. The platform will contain relevant urban resilience information and host a portfolio of search, diagnostic, scenario modelling and management tools. Moreover, the platform will include educational elements that provide a 'virtual centre of excellence', and self-assessment tools that help end-users to assess the general resilience and security level of an existing or proposed large scale infrastructure.

Within the portfolio catalogue end-users will have access to the “Harmonised Resilience Toolkit”. This suite of tools will include:

- Dynamic approaches to Risk Assessment Methodologies;
- Integration software (integrated management systems to combine previously isolated building systems);
- Design and planning guidelines for resilience of large scale urban built infrastructure;
- Socio-economic tools (includes societal acceptance and adaptive governance measures);
- Engineering/construction/retrofit tools (for best placement of sensor technologies, causal relationship analysis for non-compatible building system elements etc);
- Critical flows (sustainability) tools for energy efficiency, smart grids and multi-functionality etc);
- Educational multimedia tools (for promotion and dissemination of HARMONISE concept).

PARTNERS	COUNTRY
Future Analytics Consulting Ltd (FAC)	Ireland
Teknologian Tutkimuskeskus VTT (VTT)	Finland
University of Ulster (UU)	United Kingdom
Selex ES SPA (SXE)	Italy
Fundacion Tecnalia Research & Innovation (Tecnalia)	Spain
Bergische Universitaet Wuppertal (UW)	Germany
Lonix OY (Lonix)	Finland
Building Design Partnership Ltd. (BDP)	United Kingdom
LeighFisher Ltd. (LeighFisher)	United Kingdom
Ayuntamiento De Bilbao (Bilbao Council)	Spain
Comune di Genova (CDG)	Italy
University of Warwick (UoW)	United Kingdom

INTACT / On the Impact of Extreme Weather on Critical Infrastructures

Information

Grant Agreement N°
606799
Total Cost
€4,390,414.07
EU Contribution
€3,445,518.92
Starting Date
01/05/2014
Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO)
Safety and Security Research
Oude Waalsdorperweg 63
P.O. Box 96864, NL-2509 JG The Hague
2597 AK, The Hague, The Netherlands
Contact
Peter Petiet
Tel: +31 8886 64006
Mobile: +31 6117 00527
Fax: +31 7032 80961
E-mail: peter.petiet@tno.nl
Website:
www.intact-project.eu

Project objectives

The overall objective of the INTACT project is to offer decision support to critical infrastructure (CI) operators & policy makers regarding critical infrastructure protection (CIP) against changing extreme weather event (EWE) risks caused by climate change.

This overall objective concerns to:

» Assess regionally differentiated risk throughout Europe associated with extreme weather

» Identify and classify on a Europe-wide basis CI and to assess the resilience of such CI to the impact of EWE

» Raise awareness of decision-makers and CI operators about the challenges EW conditions may pose to their CI

» Identify potential measures and technologies to consider and implement

Description of the work

To achieve the objectives the INTACT project will:

» Collect and analyse trends, patterns and tendencies in Extreme Weather: based on recent historical trends & data, extrapolations and future scenarios for various EW types is evaluated

» Assess the risk and vulnerability of CI due to extreme weather: based on historical CI incidents, an assessment is made of future vulnerabilities due to EWE

» Develop a methodology and tools for risk management: bring together models & tools to support decision-making for long term planning and design, and/or for crisis management

» Collect, assess, augment, and disseminate best practices and measures to reduce risk: based on recent experiences and applications, while identifying current innovative and/or new technology

» Bring together the stakeholders from the various domains: climate researchers, engineers, first responders and crisis response organisations with CI owners and operators convene in workshops and case studies

» Apply and demonstrate to stakeholders the potential of the INTACT methodology for a selected set of case studies: throughout Europe and for different regional settings and EW conditions

» Develop the INTACT Reference Guide (IRG), a WIKI, based on generalised/specific datasets, scenarios and simulations integrated within the different activities of the project

Expected results

» A repository on valuable background information and knowledge about climate change, EWE, CI, with examples, illustrations and references

» Data on

- Climate change for the medium-term & long-term period
- Changes in frequency and strength of EWEs
- Changes in induced hazards (where possible)
- Specific vulnerabilities for EWE for specific CI

» Step-by-step method on how to use this data to determine the future EWE risks to your CI

- Using your own familiar current tools
- Supporting mitigation strategies and techniques

All information will be made available through the INTACT Reference Guide (IRG), in the form of a publicly accessible WIKI, http://www.intact-wiki.eu

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Centro Euro-Mediterraneo sui Cambiamenti Climatici S.c.a.r.l. (CMCC)	Italy
Stichting DELTARES (DELTARES)	The Netherlands
Future Analytics Consulting Limited (FAC)	Ireland
DRAGADOS SA (DRAGADOS)	Spain
HR Wallingford Limited (HRW)	United Kingdom
PANTEIA BV (PANTEIA)	The Netherlands
Stiftelsen Norges Geotekniske Institutt (NGI)	Norway
Agencia Estatal Consejo Superior de Investigaciones Cientificas (CSIC)	Spain
University of Ulster (ULSTER)	United Kingdom
University of Stuttgart (USTUTT)	Germany
Teknologian Tutkimuskeskus VTT (VTT)	Finland

RAIN / Risk Analysis of Infrastructure Networks in response to extreme weather

Information

Grant Agreement N°
608166
Total Cost
€4,771,603
EU Contribution
€3,493,600
Starting Date
01/05/2014
Duration
36 months

Coordinator

TRINITY COLLEGE DUBLIN (TCD)
Department of Civil, Structural and Environmental Engineering
Museum Building, Trinity College Dublin
Dublin 2 – Dublin – Ireland
Contact
Dr. Alan O'Connor
Tel: +353 1 896 1822
Mobile: +353 87 2848935
Fax: +353 1 6773072
E-mail: alan.oconnor@tcd.ie
Website: www.rain-project.eu

Project objectives

In recent years, a variety of extreme weather events have threatened and damaged many different regions across Europe and worldwide. These events can have a devastating impact on critical infrastructure systems.

RAIN's vision was to develop a systematic risk management framework that explicitly considers the impacts of extreme weather events on critical infrastructure and developed a series of mitigation tools to enhance the security of the pan-European infrastructure network. This project quantified the complex interactions between weather events and land-based infrastructure systems. RAIN facilitated a cross-European collaborative platform, supported by the necessary tools and methodologies, where relevant stakeholders can share data, results of model simulations, and operational strategies in a seamless, efficient, and effective way.

Description of the work

Transport, energy and telecommunications infrastructure were all considered and risk mitigation strategies were developed. This was achieved by developing an operational analysis framework that considered the impact of individual hazards on specific infrastructure systems, and the coupled interdependencies of critical infrastructure through robust risk and uncertainty modelling. The framework considered cascading hazards, cascading effects and time dependent vulnerabilities, with the ultimate objective of developing practical software tools and guidelines to provide support to European infrastructure managers during an extreme weather event, and to minimise the latter's impact by developing mitigation and response strategies. These tools were implemented within a novel Europe-wide operational and response strategy that emerged from this research. The ability of this response plan to cut across borders was guaranteed by the pan-European multi-disciplinary consortium.

Expected results

Technical and logistical solutions were developed to minimise the impact of extreme weather events, these included novel early warning systems, decision support tools and engineering solutions to ensure the rapid reinstatement of the infrastructure network. The outputs from the project resulted in enhanced safety and reliability of the infrastructure network in the case of major disruptions and addresses European policy in the areas of safety and security, inter-modality and emergency response planning. RAIN will aid decision-making in the long term in securing new robust infrastructure development and the protection of existing infrastructure against changing climates and increasingly more unpredictable weather patterns.

PARTNERS	COUNTRY
Trinity College Dublin (TCD)	Ireland
European Severe Storms Laboratory e.V. (ESSL)	Germany
Zilinska Univerzita V Ziline (UNIZA)	Slovakia
Delft University of Technology (TU-Delft)	The Netherlands
Gavin and Doherty Geosolutions Ltd. (GDG)	Ireland
Dragados S.A. (DSA)	Spain
Freie Universität Berlin. (FU-Berlin)	Germany
Roughan &O'Donovan (ROD)	Ireland
Hellenberg International (HI)	Finland
Institute of International Sociology of Gorizia (ISIG)	Italy
PSJ (PSJ)	The Netherlands
Finnish Meteorological Institute (FMI)	Finland
Youris.com (youris)	Italy
Independent Power Transmission Operators (IPTO)	Greece
Aplicaciones en Informatica Avanzada SL (AIA)	Spain

RIBS / Resilient infrastructure and building security

© teekid - istockphoto.com

Information

Grant Agreement N°
242497
Total Cost
€4,406,966.80
EU Contribution
€3,321,957.80
Starting Date
01/11/2010
Duration
36 months

Coordinator

UNIVERSITY COLLEGE LONDON
Department of Security and Crime Science
2 - 16 Torrington Place
WC1E 7HN, London,
UNITED KINGDOM
Contact
Dr Hervé Borrion
Tel: +44 (0) 20 3108 3194
Fax: +44 (0) 20 3108 3088
E-mail: h.borrion@ucl.ac.uk
Website: www.ribs-project.eu

Project objectives

Objective 1
To characterise a range of existing and emerging (i) security threats and (ii) protection measures, and integrate the results into a single comprehensive multi-layer model that can be used for vulnerability analysis.

Objective 2
To characterise relevant physical and non physical elements of buildings, and integrate the results into a single comprehensive multi-layer model that can be used for vulnerability analysis.

Objective 3
To design and implement an effective vulnerability analysis technique utilizing models of the “complex threat” and the “complex infrastructure” and use this technique to analyse the protection measures of an existing building.

Objective 4
To develop a method for defining suitable requirements for the design of infrastructure-specific protection measures focusing on functions such as detection, identification, and authentication.

Objective 5
To develop and apply a method for assessing the level of protection of buildings provided by additional protection measures against a range of security threats.

Objective 6
To determine, validate and promote the requested design requirements and additional physical protection measurements through a field-study involving an existing building and end-users.

Description of the work

The RIBS-project supports the design of effective and viable integrated security measures aimed at protecting infrastructures without impacting on their business dynamics. In a global context where national interests are increasingly interrelated, the most vulnerable infrastructures in Europe, and particularly the most critical ones, are primary targets for terrorists. Attacks, carried out under a national, political, or religious banner, now strike regularly in our cities, causing deaths, damage and disruption on an unprecedented scale. In the past seven years alone, 1300 terrorist incidents have taken place on European soil.

The RIBS project will deliver more effective and viable security measures by supporting a design process that integrates a broader understanding of the environment (and the contextual factors such as human elements) within which these measures are meant to be implemented.

The particular objectives of the project include a set of functional and non-functional requirements that will drive an effective security system design process, and a set of protection measurement techniques that can be used to assess the level of protection offered by candidate security products proposed to be implemented in buildings and infrastructures.

This work will be carried out for a range of security systems aimed at securing buildings against hostile reconnaissance, intruders and hazardous attack (including chemical, biological and explosive).

Expected results

The RIBS-project will derive a scientific method for security system engineering design that can be challenged and improved over the years, similarly to other areas of engineering and physical sciences. The results include:

- » Phase 1: Study of a live building and its 'eco-system', its protection measures, and threats; and integration of these elements into a single multi-layer model;

- » Phase 2: Identification of vulnerabilities through incident analysis and protection-measures analysis;

- » Phase 3: Development of design requirements.

PARTNERS	COUNTRY
UNIVERSITY COLLEGE LONDON (UCL)	United Kingdom
TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY (TECHNION)	Israel
H.PETROPOULEA&CO (2E)	Greece
KUNGLIGA TEKNISKA HOEGSKOLAN (KTH)	Sweden
DANMARKS TEKNISKE UNIVERSITET (DTU)	Denmark
EFI (Anonymised name of Partner)	Greece
Aedas Architects Limited (Aedas Architects)	United Kingdom

SECUR-ED / Secured Urban Transportation - European Demonstration

© Paolo Margari

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261605
Total Cost
€39,996,659.20
EU Contribution
€25,468,072
Starting Date
01/04/2011
End Date
30/09/2014

Coordinator

THALES COMMUNICATIONS & SECURITY SAS (THA)
AVENUE DES LOUVRESSES 4
92230 GENNEVILLIERS
FRANCE
Contact
Virginie Couderq
Tel: +33 (0)1 73 32 28 28
Fax: +33 (0)1 73 32 16 92
E-mail: Virginie.coudercq@thalesgroup.com
Website:
www.thalesgroup.com

Project objectives

SECUR-ED's rationale was to create a global European improvement in mass transportation security through the development of packaged modular solutions validated through demonstrations, and made available to the full community of operators.

SECUR-ED brought together major operators and top industrial integrators to enhance the security of urban public transportation in medium and large cities, through live demonstrations.

Based on the best practices, in a very diverse societal and legacy environment, SECUR-ED aggregated a consistent and interoperable mix of technologies and processes, covering all aspects, from risk assessment to complete training packages.

Description of the work

The project set up demonstrations in Berlin, Madrid, Milan, and Paris. Satellite demonstrations were also run in Bergen, Bilbao, Brussels, Bucharest, Izmir, and Lisbon. In all the city demonstrations the aim was the same: to increase security in mass transportation. Both people and infrastructure security were addressed by the project, as was a range of issues from minor offences to major terrorist threats, all while taking into account legal, cultural and societal environments.

A ground-up approach was taken to ensure that the solutions being proposed and demonstrated were possible and could be easily integrated into existing operational procedures. In the process, risks were identified and best practices shared.

The demonstrations provided evidence of adaptability and inter-operability of solutions for the urban transportation environment, from procedures to video-analysis, CBRN-E detection or information management, including training, cyber-security and simulation tools.

Results

The security solutions demonstrated, whether procedural or technical, were strongly influenced by the growing role of Information and Communication Technologies (ICT) in the transportation systems. But this does not change the fact that most of the assets have a life expectancy of several decades. This is why the prescriptions made generally consider their interactions with the legacy systems, as well as a future-proof vision within this same scale of time.

In public transport, where the passenger is at the same time the main beneficiary of the security measures and - together with the staff - the potential victim of resulting privacy breaches, the long-term vision of the security approach can only be based on an ethical dynamic balance between societal benefits and prevention of unnecessary intrusive methods. This balance changes rapidly with the local context, the international (security) situation or the evolution of the general use of technology.

SECUR-ED – with its 41 partners, 10 field demonstrations conducted over Europe, its wide-spectrum Advisory Groups and multiple studies conducted – has produced a wealth of results encompassed in over 50 documents.

A White Paper (available in the Downloads section of the website) draws lessons learned and makes recommendations for maximum positive impact on mass transport operators and suppliers as well as passengers, helping to improve overall quality of life.

PARTNERS	COUNTRY
THALES SECURITY SOLUTIONS & SERVICES SAS (THA)	France
ALSTOM TRANSPORT S.A. (ALS)	France
Ansaldo STS S.p.A. (ANS)	Italy
Azienda Trasporti Milanesi (ATM)	Italy
Bombardier Transportation GMBH (BOM)	Germany
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Consorcio Regional de Transportes de Madrid (CTM)	Spain
Deutsche Bahn AG (DBA)	Germany
European Organisation for Security SCRL (EOS)	Belgium
Edisoft - Empresa de servicios e desenvolvimento de software SA (EDI)	Portugal
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
HAMBURG-CONSULT Gesellschaft für Verkehrsberatung M.B.H. (HCO)	Germany
Ingenieria y Consultoria para el Control Automatico, SL (ICC)	Spain
INOV INESC INOVAÇÃO – Instituto de Novas Tecnologias (INO)	Portugal
European Commission - Joint Research Centre (JRC)	Belgium
Regia Autonoma de Tranport Bucuresti (RTB)	Romania
EMEF, SA - Empresa de Manutenção de Equipamento Ferroviário, SA (EME)	Portugal
MTRS3 Solutions and Services LTD (MTR)	Israel
NICE Systems Ltd. (NIC)	Israel
Universitaet Paderborn (UPB)	Germany
Régie Autonome des Transports Parisiens (RTP)	France
Morpho (MPH)	France
Empresa Municipal de Transportes de Madrid SA (EMT)	Spain
Ministère de l'Intérieur, de l'Outremer et des collectivités territoriales Direction de la défense et de la sécurité civile (STS)	France
Société Nationale des Chemins de Fer Français (SNF)	France
FNM SPA (FNM)	Italy
Universitetet i Stavanger (STA)	Norway
Société des Transports Intercommunaux de Bruxelles SSF (STIB)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	Netherlands
Technische Universitaet Dresden (TUD)	Germany
Union Internationale des Transports Publics - UITP (UIP)	Belgium
Union des Industries Ferroviaires Européennes - UNIFE (UNI)	Belgium
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Julius-Maximilians Universitaet Wuerzburg (WUE)	Germany
Ingenieria y Economia del Transporte S.A. (INE)	Spain
G. Team Security Ltd (GTE)	Israel
AXIS Communications Aktiebolag (AXI)	Sweden
Turkiye Cumhuriyeti Devlet Demir Yollari Isletmesi Genel Mudurlugu (TCD)	Turkey
Selex Elsag S.p.A. (SEG)	Italy

SPIRIT / Safety and Protection of built Infrastructure to Resist Integral Threats

© SPIRIT

RESEARCH COMPLETED

Information

Grant Agreement N°
242319
Total Cost
€4,885,951
EU Contribution
€3,497,684.50
Starting Date
01/08/2010
End Date
31/07/2013

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK
Physical Protection and Survivability
Lange Kleiweg 137
PO Box 45
2280 AA Rijswijk
The Netherlands
Contact
Ms Jolanda van Deursen
Tel: +31 (0) 888 66 1289
Mobile: +31 (0) 630 72 7331
Fax: +31 (0) 888 66 6932
E-mail: Jolanda.vandeursen@tno.nl
Website: www.infrastructure-protection.org

Project objectives

The project SPIRIT (Safety and Protection of built Infrastructure to Resist Integral Threats) is a capability project. The aim of this project is to provide the technology and know-how for the protection of buildings and people against terrorist threats and to minimize the consequences of a terrorist attack in terms of number of casualties/injuries, damage and loss of functionality and services, by providing:

- » tools to quantify the vulnerability of built infrastructure;
- » a portfolio of protective products;
- » a guidance tool for safety based engineering to realize a required built infrastructure protection and resilience level;
- » a proposal on how to take a CBRE-threat into account in the building guidelines.

Description of the work

Terrorist attacks with explosives (E) or chemical, biological or radiological (CBR) agents are threats with a low probability but with disastrous consequences. People, critical infrastructures and utilities have to be protected. The societal community should not be disrupted by acts of terrorism.

SPIRIT works on solutions to realize sufficient resilience of the urban infrastructure for rare occasions with minimum effect on normality. Hitherto, normal regulations and building guidelines do not take into account the CBRE threat.

The required specialist knowledge on explosion dynamics, response of structures, dispersions of toxic agents and injuries is available within the SPIRIT Consortium. Making this knowledge available and finding solutions that can be integrated into normal planning and building procedures is part of the work to be carried out.

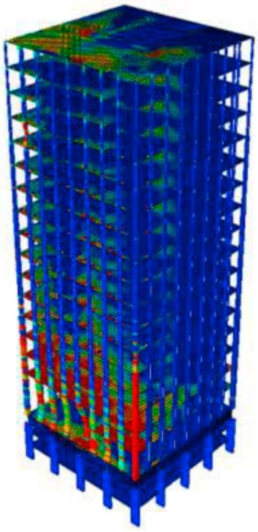
Results

The scope of SPIRIT concerned resilience against CBRE terrorist threats to large modern buildings where significant numbers of people may be present. Based on a preliminary threat assessment, a representative range of potential scenarios (20 chemical, 12 biological, 9 radiological and 14 explosive) was defined. Together with two concrete buildings whose structures are typical of urban landscapes, these scenarios formed the basis for the quantitative vulnerability study carried out by the project.

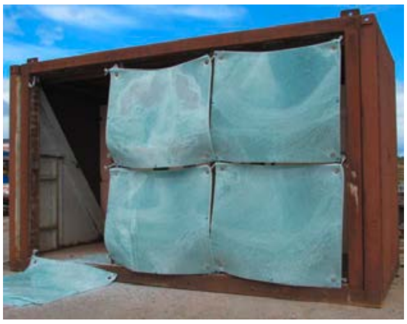
Extensive damage and consequence calculations (including loading predictions, dispersion calculations, injury and lethality predictions and finite element simulations) were performed to generate a database of results. These extend beyond the initially defined scenarios and buildings, offering options for applying the results to additional threats and structures.

With regard to the protective solutions, multiple tests and extensive assessments were conducted, thus yielding quantitative information about the protection level provided by the tested products. Designs of the studied protection products were improved and optimized, and their costs were studied. Other available protective solutions were identified through: internet searches, the previous experience of consortium members and expo visits. All available information is gathered in a portfolio of protection products.

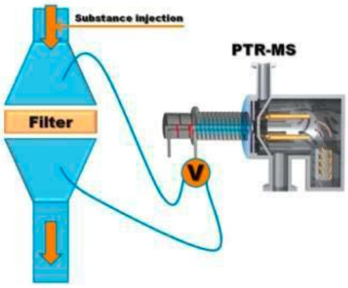
Recommendations for a regulatory framework and a guidance tool were also developed based on the risk assessment methodology, consequence models and data obtained. The guidance tool enables a user to quantitatively estimate the risks and consequences of chemical, biological, radiological and explosion (CBRE) attacks on new or existing buildings and to optimize their protective design. There are two versions of the guidance tool: a publically available demo version and the classified full tool.



Numerical simulation



Blast testing of glazing



Filter and detection system for C-threats

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Schüßler-Plan Engineers Ltd (SP)	Poland
Arup Group Ltd (ARUP)	United Kingdom
Hamilton Erskine Ltd (HE)	United Kingdom
Artemis control AG (ART)	Switzerland
Ducon GmbH (DUC)	Germany
Ionicon Analytik GmbH (ION)	Austria
Corsmit Raadgevend Ingenieurs BV (CORS)	The Netherlands
European Commission - Joint Research Centre (JRC)	Italy

VASCO / Virtual Studio for Security Concepts and Operations

Information

Grant Agreement N°
607737
Total Cost
€4,151,940.00
EU Contribution
€3,037,341.00
Starting Date
01/03/2014
Duration
36 months

Coordinator

DIGINEXT (DXT)
RTD Department / Simulation and Virtual Reality Division
ZAC de la Grande Plaine
5, rue Brindejonc des Moulinais
BP 15872
31506 TOULOUSE Cedex 5
FRANCE
Contact
Stéphane Collins
Tel: +33 5 61 17 66 66
Fax: +33 5 61 17 65 78
E-mail:
stephane.collins@diginext.fr
Website:
http://vasco.diginext.fr/

Project objectives

The concentrated localisation of government buildings and critical infrastructure sites, within or close to dense urban environments, is a source of serious security risks that are hard to anticipate: attacks on consulates and embassies, violent demonstrations near parliamentary buildings; attacks on government buildings or educational institutions; or the paralysing effects of natural disasters.

VASCO aims to:

1. develop a system to enable security professionals to construct and assess security concepts and measures, leading to an evidence-based, all-risk approach for the protection of government buildings of critical importance;
2. build a knowledge and best practice database to capture dynamic and visual reference scenarios based on VASCO's work.

VASCO will offer security experts:

- a realistic visual representation of buildings within an urban environment, combining geographic details (roads, nearby buildings of potential relevance, critical infrastructures) with architectural information (lay-out of the building, exits, windows, garden entrances, roof top access, parking garage etc.);
- capabilities to create dynamic scenarios, allowing security experts to employ their toolbox of virtual security devices (e.g. cameras, sensors) and security personnel in the virtual environment, and to simulate their behaviour and assess their effectiveness.

Description of the work

VASCO will develop the following:

- a new-generation tool based on "serious game" principles and using the latest technologies for the study and assessment of security concepts and measures related to the protection of government building;
- an automated software solution for rapidly reconstructing digital 3D mock-ups of buildings, including interiors from a series of photographs;
- simulation capabilities to help users create dynamic scenarios that identify resources (e.g. security equipment and units), strategies, events, and threats ;
- new interaction techniques such as tangible interfaces coupled with multitouch multiuser surfaces;
- a VASCO software developer kit to enable third-parties to extend the system by implementing additional modules or gateways to other services and simulators;
- the ability of the whole system to run on entry-level PCs or laptops, with the appropriate graphic board and hard drive.

Expected results

VASCO will help complete the product line for security and crisis management developed by DIGINEXT in the frame of the CRIMSON and INDIGO EC projects (http://crimson.diginext.fr, http://indigo.diginext.fr).

VASCO's expected results will:

- » enable users to rapidly and cheaply create a 3D digital model of a building, including interiors, and its environment from series of photographs;
- » offer a natural user interface, based on a set of real objects (e.g. rulers, pencils, erasers) to be used in conjunction with a multitouch multiuser table. This will allow users to intuitively edit the DMU, control simulations, or make annotations and measurements without having to learn a software user interface;
- » enable the creation and simulation of custom-made event- and threat-scenarios such as hostage-takings, fire, earthquakes and demonstrations, bomb blasting and architectural damages – and the response to these;
- » sensitize decision-makers, security teams and building owners to the security issues related to critical structures in dense urban environments through visual and educational scenarios;
- » allow use of visual reference scenarios to study and assess new security concepts, which are stored in a knowledge database. The latter will hold a wide variety of security concepts whose scenarios users can manipulate to test certain security concepts while holding other features constant. Thus, managers will be able to search the database for feasible strategies and learn from the experiences of other users. This will encourage users to store scenarios – fictitious and real – together with assessed security concepts. Future users will be able to access the scenario and the concepts, watching with detailed precision how a given threat evolved and what was done (or not) to counter it;

PARTNERS	COUNTRY
DIGINEXT SARL (DXT)	France
Consiglio Nazionale Delle Ricerche (CNR)	Italy
Centro Di Ricerca, Sviluppo E Studi Superiori In Sardegna (CRS4)	Italy
Immersion Sas (ISA)	France
Center For Security Studies (KEMEA)	Greece
Crisisplan B.V. (CRISP)	The Netherlands
Försvarshögskolan, Swedish National Defence College (CRISM)	Sweden

VITRUV / Vulnerability Identification Tools for Resilience Enhancements of Urban Environments

© VITRUV

Information

Grant Agreement N°
261741
Total Cost
€4,520,921.80
EU Contribution
€3,339,898
Starting Date
01/05/2011
Duration
36 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V
Fraunhofer EMI
Hansastrasse 27c
80686 Germany
Contact
Dr. Werner Riedel
Tel: +49 7628 9050 692
Fax: +49 7628 9050 677
E-mail: werner.riedel@emi.fraunhofer.de
Website:
www.emi.fraunhofer.de

Project objectives

With half of the world's population currently living in urban centres, the security of citizens is of paramount importance and a growing concern. Thus, urban planning practice must incorporate appropriate security measures for vulnerability identification and resilience enhancements. Currently no software tool exists that enables urban planners to take these aspects into consideration.

The objective of VITRUV is the development of software tools that can be used for the long and complex urban planning process. These tools address three different detail levels. Based on an all hazard risk approach, the tools will enable planners:

» to make well-considered systematic qualitative decisions (concept level);

» to analyse the susceptibility of urban spaces (e.g. building types, squares, public transport) with respect to new threats (plan level); and

» to perform vulnerability analyses of urban spaces by computing the likely damage on individuals, buildings, traffic infrastructure (detail level).

Description of the work

Based on urban planner requirements, including financial and procedural limitations and preferences, tools will be developed on three different detail levels.

On the concept level, an overarching methodology will be developed to generate suitable city planning alternatives. A computer support tool will assist the use of this method.

On more detailed levels, algorithms are developed to determine weak points in urban environments. On the plan level, this will be achieved by the use of a database of terrorist attacks and expert judgement using empirical risk analysis. This analysis can be used for a quick susceptibility and risk assessment. The second analysis will be at the detail level. Here an automated (hidden) definition of a larger number of possible attack events will be encoded in algorithms and used to assess repeatedly the damage to different urban assets (building / infrastructure types, their structural members, load bearing concepts and functions). The detail level corresponds to an automated vulnerability analysis in technical terms and is based on quantitative risk analysis sizes. Hazard and damage analysis sizes will be computed for explosive, biological and chemical threats.

Case studies will be used to support the development of the tools as well as for the extended testing and evaluation of the results in the project.

Expected results

Within the VITRUV project, tools on three different levels (concept, plan and detail) are developed that will contribute to enabling the development of more robust and resilient space in the field of urban (re)planning/(re)design/(re)engineering. Planners who use VITRUV's tools will be able to develop urban space which is less prone to and less affected by attacks and disasters, thus sustainably improving the security of the citizens.

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung E.V (Fraunhofer-EMI)	Germany
Crabbe Consulting Ltd (CCLD)	United Kingdom
Provincia di Bologna (BOLOGNA)	Italy
West Yorkshire Police Authority (WYP)	United Kingdom
Schussler-Plan Ingenieurgesellschaft mbH (SP)	Germany
Dissing+Weitling Arkitektfirma A/S (D+W)	Denmark
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	Netherlands
Downey Hynes Limited (DHP)	Ireland
Sigmund Freud Privatuniversitat Wien GmbH (SFU-CEUSS)	Austria
Decisio BV (DECISIO)	Netherlands
Thales Security Solutions & Services SAS (THALES)	France
London Borough of Southwark (SOUTHWARK)	United Kingdom

AFTER / A Framework for electrical power sysTems vulnerability identification, dEfence and Restoration

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261788
Total Cost
€4,920,367.07
EU Contribution
€3,354,193.93
Starting Date
01/09/2011
End Date
31/12/2014

Coordinator

RICERCA SUL SISTEMA ENERGETICO (RSE S.P.A.)
Via Rubattino 54
20134 – Milano - Italy
Contact
Emanuele Ciapessoni
Tel: +39 02 3992 5766
Mobile: +39 366 6352 682
Fax: +39 02 3992 5597
E-mail:
ciapessoni@rse-web.it
Website: www.rse-web.it

Project objectives

AFTER focused on the physical security and operational security of power systems, dealing with high impact, multiple contingencies and cascading events, defence actions and service restoration due to catastrophic outages.

Description of the work

Project objectives were addressed by defining a framework, methodologies, tools and techniques to evaluate and enhance the security and resilience of complex energy systems, in particular for:

- risk assessment (hazard, vulnerability and impact analysis);
- global defence and restoration.

Results

Global vulnerability analysis and risk assessment of power systems: considering the possible threats (natural vs. man-related; internal vs. external; intentional vs. unintentional). The framework allows individuals to identify critical contingencies and to quantify their impacts and risks.

Physical security improvement, by innovative techniques for early warning: to detect and to provide early warning signs of physical intrusions into substations. The tool can suggest operational practices to limit the impact of intrusions on the grid.

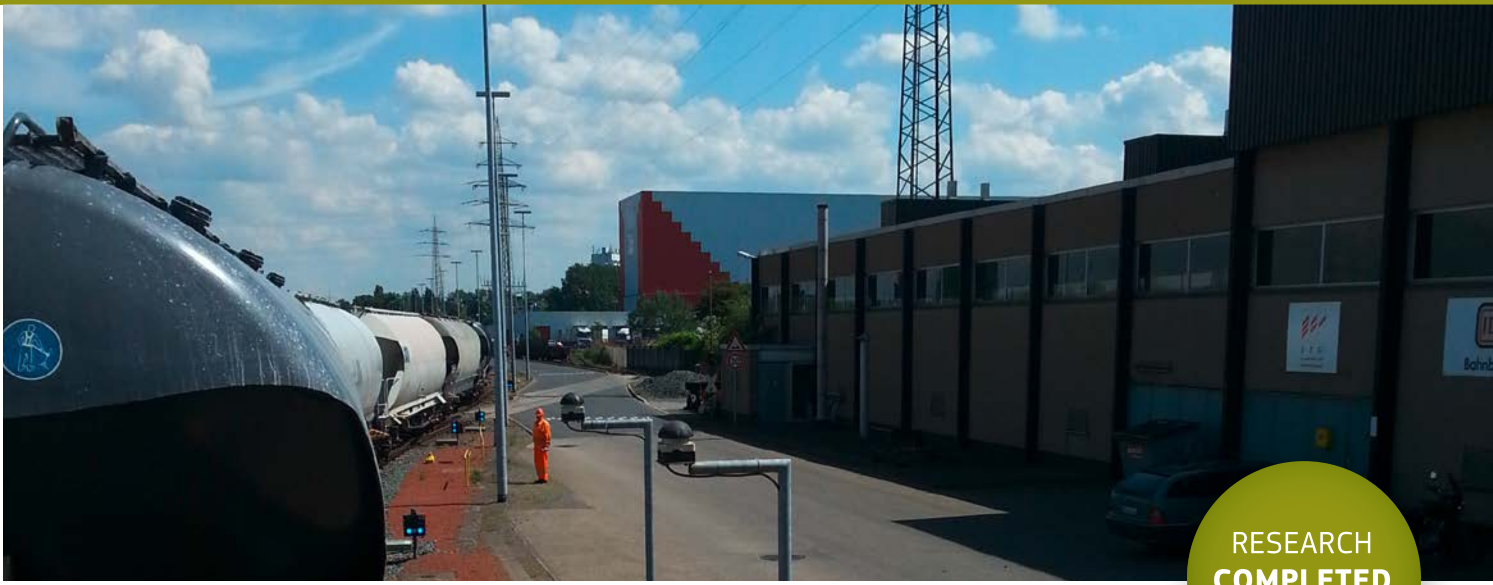
Advanced defense of power system operation following severe grid outages, by innovative defence plans techniques: to mitigate the risk of power system blackouts. The support tool integrates a security assessment with a case-based reasoning algorithm to find an appropriate emergency control action.

System restoration after major disruptions, by adaptive and efficient restoration plans: the restoration support tool, based on generic restoration milestones, allows minimisation for the restoration time by an adaptive construction of restoration strategies.

AFTER's results will affect the way security and resilience of complex interconnected energy networks are assessed, with resulting increased exploitation of transmission grids, reduction of blackout occurrence, extension and duration. Defence approaches may be exploited by manufacturers, moving to commercial solutions for TSOs. AFTER helped carry the discussion on the risk concept to TSO level, paving the way for the introduction of risk approaches in operation.

PARTNERS	COUNTRY
Ricerca sul Sistema Energetico - RSE SpA (RSE)	Italy
Agenzia nazionale per le nuove tecnologie,l'energia e lo sviluppo economico sostenibile (ENEA)	Italy
Sintef Energi AS (SINTEF-EN)	Norway
Stiftelsen Sintef (SINTEF-ICT)	Norway
Universita degli Studi Di Genova (UNIGE)	Italy
University College Dublin, National University Of Ireland, Dublin Nuid (UCD)	Ireland
The City University (CU)	United Kingdom
Alstom Power Systems SA (ALSTOM Power)	France
SIEMENS AG (SIEMENS)	Germany
JRC -Joint Research Centre- European Commission (JRC)	Belgium
ELIA SYSTEM OPERATOR (ELIA)	Belgium
TERNA - Rete Elettrica Nazionale SpA (TERNA)	Italy
CEPS AS (CEPS)	Czech Republic
ALSTOM GRID SAS (AlstomGrid)	France

CARONTE / Creating an Agenda for Research On Transportation sEcurity



RESEARCH **COMPLETED**

Information

Grant Agreement N°
606967
Total Cost
€1,376,260.00
EU Contribution
€1,256,874.00
Starting Date
01/09/2014
End Date
28/02/2016

Coordinator

FRAUNHOFER GESELLSCHAFT ZU FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. - FRAUNHOFER
Institute for Material Flow and Logistics
Hansastrasse 27c
80686 München
Contact
Joachim Kochsiek
Tel: +49 231 9743 395
Mobile: +49 173 29 55 221
Fax: +49 231 9743 77 395
E-mail: Joachim.Kochsiek.iml.fraunhofer.de

Project objectives

The objective of the CARONTE project is to provide an answer to the question of what type of security related projects should be planned to respond to current and future threats facing land transport. This includes an analysis about current or planned approaches and their introduction and effectiveness level.

Description of the work

The project is divided into seven workpackages, including project management and dissemination. In WP2 and WP3 the state of the art frameworks in land transport and its security are analyzed while emerging risks and the development of security related dangers are identified. After the initial phase gaps for land transport security are identified, potential solutions and approaches to fill identified gaps are developed. In the final work-package the research agenda is elaborated. The complete work is analyzed by desk-researchers and the partners, expert interviews and workshops and consultation of a high-level-advisory-board.

Results

The main result will be a research agenda naming the important topics for future research on EU levels to improve land transportation security. It will include a road-map for the timing of the activities.

The Research Agenda will show how to build up European capabilities to ensure security in land transportation in an efficient way and how to avoid mitigating consequences in case of incidence. It will also provide global guidelines on enhancing the surveillance of the land transport infrastructure.

Specifically, the following aspects will be elaborated:

» analyzing and describing the state of play in transport modes, including infrastructure, vehicles, processes and stakeholders, covering passenger and freight transport

» identifying and assessing potential and future risks including cyber-attacks, ICT security and covering terrorism and crime among others

» identifying potential and future gaps in security vs. security measures taken, regulations existing and planned plus current research and its foreseen results

» assessing the gaps identified and highlighting the needs for action

» analysing social and ethical aspects of security measures (human rights, privacy vs. security)

» reviewing and analyzing past and current research projects, their results and impacts on future security frames (which gaps could already be closed)

- respecting effects and frames on and from the Charter of Fundamental Rights of the European Union

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung - Fraunhofer	Germany
Austrian Institute of Technology GmbH - AIT	Austria
Vienna Centre for Societal Security - VICESSE	Austria
Loughborough University – LUNI	United Kingdom
SECEUR SPRL	Belgium
Fundación Tecnalia Research & Innovation - TECNALIA	Spain
Szechenyi Istvan University - SZE	Hungary
Institut Français des sciences et technologies des transports, de l'aménagement et des réseaux – IFSTTAR	France
Instituto tecnológico del embalaje, transporte y logística - ITENE	Spain
The University of Security Management in Košice – VSBM	Slovakia
European rail Research Network of Excellence - EURNEX e. V.	Germany

COPRA / Comprehensive European Approach to the Protection of Civil Aviation

© Kristian Peetz - Fotolia.com

Information

Grant Agreement N°
261651
Total Cost
€1,303,301.80
EU Contribution
€986,382
Starting Date
01/09/2011
Duration
18 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Ernst-Mach-Institut (EMI)
Hansastr. 27c
80686 Munich
Germany
Contact
Dr. Tobias Leismann
Tel: +49 761 2714 402
Mobile: +49 170 769 5101
Fax: +49 761 2714 1402
E-mail: Tobias.Leismann@emi.fraunhofer.de
Website: www.emi.fraunhofer.de

Project objectives

Provide the European Commission and Member States with clear guidelines for future RTD activities:

» Compilation of a comprehensive overview of end-user and customer aviation security requirements including boundary conditions like legislation and standardization issues;

» Analysis of new and emerging threats to aviation security using an all-hazard approach. Development of a hierarchy of threats reflecting factors like impact, likelihood and timescale of threats to become relevant for Europe;

» Identification of current and future security technologies taking into account new operational procedures mitigating the new threats;

» Systematic analysis and combination of technologies and procedures into holistic security concepts including organizational paradigms, social acceptability and cost-benefit aspects;

» Creation of a roadmap of the European requirements on future aviation security research and recommendations for standardization, test and certification issues.

Description of the work

Preparedness and protection against new threats while ideally improving the protection of passenger privacy, mobility and public acceptability in the future aviation security system strongly depends on the changing requirements of the stakeholders involved as well as the legal context in the European Union.

Workpackage 1 (WP1) will analyse these requirements (mid-term trends). The starting point is the state of the art description of the security systems. Further, the European legislative context will be described (preparation of standardization questions).

WP2 will identify present, new and emerging threats with impact on the future. Information will be gathered from previous and ongoing European and national research projects. It will also consider new developments for an all-hazard approach to providing a comprehensive prioritized list (e.g. destructive impact, availability) of threats to the aviation system.

WP3 will collect and analyse present security technologies and opportunities arising from new technologies (by state of development, required development costs, maturity and cost estimations of the measures). New concepts (technologies, processes) will be depicted.

WP1, WP2, and WP3 results will be merged in WP4: stakeholder requirements, threats and security solutions will be brought together into a multi-criteria analysis to assess security concepts. Assessment factors: cost-benefit analysis, socio-cultural acceptance and privacy issues, the European legal framework and standards, possible synergistic effects between security concepts and aviation development in general.

In WP5 the results of WP4 will be translated into a research roadmap and recommendations for future RTD activities.

Management (communication/reporting to European Commission, workshop planning) of COPRA is performed in WP6.

The WPs will be supported by expert groups in workshops (WS). WP1 and WP2 through workshop WS1. WP3 will be supported in WS2. WP4 will start with the output of WS2. WP5 results will be presented in WS3.

Expected results

- a comprehensive list of threats to the aviation system through an all-hazard approach;
- a catalogue of security technolgies;
- a roadmap of the European requirements for future aviation security research;
- recommendations for standardization, test and certification issues.

This all takes into account passenger privacy, mobility, public acceptability, stakeholder requirements and the legal context of the European Union.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
European Business School (EBS)	Germany
Airbus S.A.S. (AIR)	France
European Organisation for Security (EOS)	Belgium
Fraport AG Frankfurt Airport Services Worldwide (FRA)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Morpho (MPH)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Smith Heimann GmbH (SMI)	Germany
University of Ljubljana (UL)	Slovenia
KLM – Royal Dutch Airlines NV (KLM)	The Netherlands

CWIT / Countering WEEE Illegal Trade

RESEARCH **COMPLETED**

Information

Grant Agreement N°
312605
Total Cost
€1,868,303
EU Contribution
€1,868,303
Starting Date
01/09/2013
End Date
31/08/2015

Coordinator

INTERNATIONAL CRIMINAL POLICE ORGANISATION (INTERPOL)
Environmental Security Sub Directorate
INTERPOL General Secretariat
200 Quai Charles de Gaulle
69006 Lyon, France
Contact
Laurent GROSSE
Executive Director,
Resource Management
Tel: +33 472 44 70 88
E-mail: l.grosse@interpol.int
David HIGGINS
Assistant Director,
Environmental Security
Sub-Directorate
Tel: +33 472 44 76 23
Fax: +33 472 44 73 51
E-mail: d.higgins@interpol.int
Therese SHRYANE
CWIT Project Coordinator
Tel: +33 472 44 71 60
Fax: +33 472 44 73 51
E-mail: t.shryane@interpol.int
Website: www.cwitproject.eu

Project objectives

The aim of the CWIT – Countering WEEE Illegal Trade – project was to provide a set of recommendations to support the European Commission, law enforcement authorities, and customs organizations, countering the illegal trade of e-waste/WEEE (waste electrical and electronic equipment or e-waste) in and from Europe. The project collected, studied and identified gaps in the current legislation in place at the International and European level.

Only around 3 million tons of an estimated total of 8 million tons in WEEE was officially collected, treated, and reported to authorities across Europe in 2010. WEEE contains materials such as gold, copper, and palladium which makes it very valuable on the black market; attracting not just illegal single operators but serious organised crime groups. However this waste also contains hazardous substances such as mercury and cadmium.

The CWIT project was established to identify the policy, regulatory, procedural, and technical gaps as observed in today's business environment, and to suggest tangible improvements.

Description of the work

Gap analysis

The project collected, studied, and identified gaps in the current legislation at the international and European level:

» The Directive on Waste Electrical and Electronic Equipment (WEEE) (Recast) WEEE Directive 2012/19

» The Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Directive Recast 2011/65/EU

» Regulation 1013/2006 on Shipments of Waste

Illegal trade

In addition, the CWIT project carried out intensive data collection and an intelligence-based approach to:

» analyse the involvement of organized crime in the global distribution of WEEE;

» analyse criminal activity and crime types associated with illegal WEEE shipments, drawing on other work carried out to target illegal e-waste exports on an international scale;

» estimate the true volume of WEEE generated and the amounts inappropriately disposed of;

» assess the typology of companies (and brokers) involved in the export market and identifying those with a criminal history; and

» develop a detailed understanding of the destinations and routes used to carry illegal shipments.

Expected results

The Countering WEEE Illegal Trade (CWIT) project found that in EU, only 35% (3.3 million tons) of all the e-waste discarded in 2012, ended up in the officially reported amounts of collection and recycling systems.

The other 65% (6.15 million tons) was either:

- exported (1.5 million tons),
- recycled under non-compliant conditions in Europe (3.15 million tons),
- scavenged for valuable parts (750,000 tons), or
- thrown in waste bins (750,000 tons).

4.65 million tons were wrongfully mismanaged or illegally traded within Europe itself. The scavenging of products and components and the theft of valuable parts such as circuit boards and precious metals generate a serious economic loss. The intrinsic value of materials not available for compliant processing in Europe is between €800 million and €1,7 billion.

Better guidelines are required to distinguish used, non-waste electronic and electrical equipment from WEEE. In addition, an EU-wide ban on cash transactions in the scrap metal trade would also contribute to improving traceability. Organised crime is involved in illegal waste supply chains in some Member States. However, suspicions of the involvement of organised crime in WEEE are not corroborated by current information. Increased investigative processes and intelligence will lead to a

PARTNERS	COUNTRY
International Criminal Police Organization (INTERPOL)	France
WEEE Forum	Belgium
United Nations University (UNU)	Japan
Zanasi & Partners	Italy
Compliance & Risks	Ireland
Cross Border Research Association (CBRA)	Switzerland
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Italy

DEMASST / Demo for mass transportation security: roadmapping study

© NZ photo - Fotolia.com

Information

Grant Agreement N°
218264
Total Cost
€1,840,549.50
EU Contribution
€956,558.96
Starting Date
12/01/2009
End Date
11/05/2010

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Division of Defence Analysis
SE-16490 Stockholm
Sweden
Contact
E. Anders Eriksson
Tel: +46 8 5550 3747
Mobile: +46 709 277 281
Fax: +46 8 5550 3866
E-mail:
e.anders.eriksson@foi.se
Website:
http://www.demasst.eu

Project objectives

A so-called 'phase one' road-mapping project, DEMASST's goal was to identify the research priorities for a subsequent 'phase two' large scale Demonstration research project in supply chain security.

DEMASST's work aimed at three unique but mutually informative research goals, namely to develop:

- potentially innovative policy instruments, notably in view of the varying degrees of maturity and fragmentation of different national and sectoral areas;
- a road-mapping methodology for the Demo project, notably in the form of system-of-systems models and criteria grids for prioritisation of potential demo tasks;
- a specific road-map for general European mass transport security.

Results

DEMASST set out to articulate an in-depth understanding of 'system-of-systems' approaches to modern transport infrastructure. Mass transportation security was characterised by the DEMASST consortium as a fragmented physical environment, with a multitude of principal actors (i.e. public and private), and no single complete authority or control over the system as a whole. The general public was also identified as the primary end user.

By focusing on these areas, the project developed a series of criteria and analysis frameworks for deciding which tasks and capabilities in mass transportation security require attention from the Demo. Criteria included cost effectiveness, adaptability/applicability to transport security and the social and legal acceptability of a measure.

These were contrasted against a range of tasks in transport security, from situation awareness and command and control to training and staff factors. The tasks were then compared to the three criteria areas in three potential scenarios:

- terrorists who aim to place hazardous material (e.g. a home-made explosive or fire-bomb) in a densely populated area in a mass transport system;
- conflicts between opposing gangs (e.g. football hooligans), which possibly escalate to a fight;
- a mentally disturbed person with a dangerous object (e.g. a knife).

Using a scoring system developed for this purpose, it was concluded that the following task areas should be the focus of the phase two Demo:

» risk assessment-based command and control capabilities;

» interoperability and information interfaces;

» learning and training;

» threat identification and detection capabilities;

» tracking and identification;

» early intervention.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Ansaldo STS (ANSALDO)	Italy
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
EADS Astrium (Astrium)	France
Forsvarets forskningsinstitutt (FFI)	Norway
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-INT)	Germany
Ingeniería y Economía del Transporte SA (INECO)	Spain
Stiftelsen SINTEF (SINTEF)	Norway
Fundación Inasmet (TECNALIA-INAS)	Spain
Thales Security Solutions & Services SAS (T3S)	France
Tecnologia E Investigacion Ferroviaria S.A. (TIFSA)	Spain
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland

DITSEF / Digital & innovative technologies for security & efficiency of first responder operations

© sonya etchison - Fotolia.com

Information

Grant Agreement N°
225404
Total Cost
€4,180,383.81
EU Contribution
€2,798,517.50
Starting Date
01/01/2010
Duration
36 months

Coordinator

SAGEM DEFENSE SECURITE
Le Ponant de Paris
27 Rue Leblanc
F-75512 Paris Cedex 15
France
Contact
Philippe Clément
Tel: +33 1 69 19 94 85
E-mail: Philippe.clement@sagem.com
Website: http://www.ditsef.eu/

Project objectives

One of the main problems of First Responders (FR) (fire fighters, police, etc.) in the case of a crisis occurring at critical infrastructures is the availability of relevant information for the First Responder itself and for the local manager. The loss of communication and location, the lack of information concerning the environment (temperature, hazardous gases, etc.) and the poor efficiency of the Human Machine Interface (HMI) on the FR side are the main current drawbacks. Therefore, during the intervention there is a gap between the First Responders' situation (positioning, health, etc.) and the overall overview at their mobile headquarters.

DITSEF aims at increasing the effectiveness and safety of First Responders through optimal information gathering and sharing with their higher command levels.

Description of the work

The DITSEF project is organised in a number of sub projects and 5 workshops:

» *First Workshop:* The first workshop is dedicated to the common and usual scenarios which drive FR interventions (analysis of potential threats, typical emergency operations with a definition of the role of FRs according to their defined missions);

» *End-user inputs:* Presentation of some typical infrastructures (arrangement of the buildings, legal constraints, emergency measures) and of typical iinterventions of FRs;

» *Second Workshop:* Discussion and analysis of the technical and functional requirement issues;

» *End-user inputs:* classification of expected functional requirements in line with defined scenarios;

» *Third Workshop:* Presentation by the consortium of the selected technologies (innovated and/or improved);

» *End-user inputs:* Analysis and Classification of the most valuable future technical solutions proposed by R&D;

» *Fourth Workshop:* Presentation of innovative results proposed by R&D;

» *End-user inputs:* Analysis and comments with the R&D team regarding the proposed solutions and first view of the integration in a systemic approach;

» *Fifth Workshop:* Demonstration with FR in a concrete site and scenario;

» *End-users inputs:* Discussion on future needs and research plan experimentation and demonstration program.

Expected results

The DITSEF project will provide solutions in four areas:

- Communication;
- Indoor localisation;
- Sensors;
- Human Machine Interface.

The aim of the project is to propose to integrate these technologies into a system through scenarios validated by the end users.

These new technologies must respond to the end user's needs.

PARTNERS	COUNTRY
Sagem Défense Sécurité (SDS)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Cassidian S.A.S. (EADS)	France
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Elsag Datamat spa (ED)	Italy
National Centre for Scientific Research "Demokritos" (DEM)	Greece
INFITHEON Technologies Ltd (INFI)	Greece
T - SOFT spol. s r.o. Praha (TSOFT)	Czech Republic
National Civil Protection Service Directorate General (MES-TDCP)	Bulgaria
SELEX Sistemi Integrati S.p.A. (SSI)	Italy

EURACOM / EUropean Risk Assessment and COntingency planning Methodologies for interconnected networks

© EURACOM

RESEARCH COMPLETED

Information

Grant Agreement N°
225579
Total Cost
€1,038,290
EU Contribution
€833,860
Starting Date
01/07/2009
End Date
31/03/2011

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Contact
Sophie Batas
E-mail:
Sophie.batas@eos-eu.com
Website:
www.euracom-project.eu

Project objectives

EURACOM addressed the issue of protection and resilience of energy supply for Europe's interconnected energy networks. Its objective was to identify, together with European critical energy infrastructure operators, a common and holistic approach (based on an 'end-to-end energy supply chain' concept) for risk assessment and risk management solutions.

By establishing links and coherent risk management procedures across energy sectors and EU countries, the resilience of critical energy services across the whole energy infrastructure chain should increase.

Results

In order to develop a common European methodology for risk management and contingency planning, the project began with a research framework to analyse energy networks and their critical elements. This led to two studies of:

» existing risk assessment methodologies, which took stock and analyzed available international and European guidelines and good practices for risk assessment across the whole energy infrastructure chain;

» common areas of contingency planning methodologies, which provided a review of current business continuity management (BCM) practices from various sources. This encompassed international, national and domain-specific standards and guidelines.

The result was a methodology that proposes principles for a wider and consistent adoption of risk assessment and contingency planning approaches in the energy sector. EURACOM's draft outline for a common methodology is available at: https://circa.europa.eu/Members/irc/securejrc/jrc_euracom/home

EURACOM also created a common platform for discussion and future decision-making at European level across all stakeholders of the energy chain. In addition to five stakeholder workshops, the project set up a permanent networking forum. This restricted website offers energy infrastructure stakeholders a place to share their risk management experiences.

EURACOM's findings, including the common methodology, will be fed into policy discussion at EU level, with the long-term goal of incorporating these practices into EU regulatory requirements to encourage further analysis of the legal, technological (especially cyber) and economic implications of common risk management across Europe.

PARTNERS	COUNTRY
European Organisation for Security (EOS)	EU
Altran Technologies SA (ALTRAN)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
European Commission - Joint Research Centre (JRC)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Thales e-Security Ltd (THALES)	United Kingdom
Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)	Portugal

EUROSKY / Single European Secure Air-cargo Space

© Eurosky

Information

Grant Agreement N°
312649
Total Cost
€19,086,960.06
EU Contribution
€11,708,124
Starting Date
01/05/2013
Duration
48 months

Coordinator

BMT GROUP LTD (BMT)
Research Directorate
Goodrich House,
1 Waldegrave Road
TW11 8LZ – Teddington
UK
Contact
Dr Fernando Caldeira-Saraiva
Tel: +44 208 6144 244
Mobile: +44 7785 310 334
Fax: +44 208 977 9304
E-mail:
fernando@bmtmail.com
Website:
www.euroskyproject.eu

Project objectives

EUROSKY will deliver a high impact programme for improved air-cargo security and facilitation to safeguard international supply chains and the security of citizens whilst fostering international co-operation and a broad stakeholder engagement from all segments of the industry. The main project objectives are to:

a. provide systemic solutions for European air cargo security that addressi prevailing complexities and vulnerabilities aligned with international initiatives, while building on complementary on-going projects

b. offer different stakeholder groups enhanced capabilities for integrating preventive and reactive controls that address their threats in a timely and effective manner with optimised cost

c. secure air cargo supply chains whilst facilitating the overall process (i.e. achieving security without stoppages, keeping the cargo movements unimpeded at all times).

Description of the work

Requirements analysis from security, legal, policy, market and technology perspectives will be undertaken and guided initially by the EUROSKY Demonstrators. Subsequently, stakeholder surveys and workshops will be used to broaden the coverage. An important outcome will be a detailed survey of security gaps and threats across the complete air cargo supply chain.

The results of the requirements analysis will be used to produce the EUROSKY blueprints. These will address:

» integrated model of air-cargo security management including an air-cargo threat taxonomy

» operational model for detection and targeting/detection prioritization

» supervisory strategic management model

The EUROSKY solutions (Next Generation Screening Solutions, EUROSKY Ecosystem and Integrated Air-cargo Security Solutions) will be produced during the second year by leveraging the complementary competencies of the consortium partners and outputs from other related projects.

The Demonstrators will be used to validate the EUROSKY solutions under realistic conditions, to ascertain feasibility and benefits of the solutions and to provide feedback for improvements.

Expected results

EUROSKY will raise the bar in air cargo security to safeguard international supply chains and the security of citizens in general and that of air travellers across European states by: a comprehensive list of threats to the aviation system through an all-hazard approach;

» contributing to the development of a unified European aviation security approach in a global supply chain context - the 'Single European Secure Air-cargo Space';

» developing a strategic set of effective innovative measures (concepts, processes, technologies), centred on next-generation detection systems, to improve security whilst maintaining flows and optimising costs.

EUROSKY will:

1.Support European and international programmes aimed at:

a. Establishing a common approach and associated infrastructure for international co-operation and for enforcing air-security regulations and risk-based approaches in a uniform manner across the EU States;

b. Specifying detection technology requirements and future research areas;

c. Monitoring the effectiveness of regulations, standards and enforcement controls to fuel continuous improvement;

d. Managing changes, due to new or updated regulations, in a timely and cost effective manner.

2. Provide innovative aviation security solutions to implement EU policy addressing requirements from different industry stakeholder groups, including:

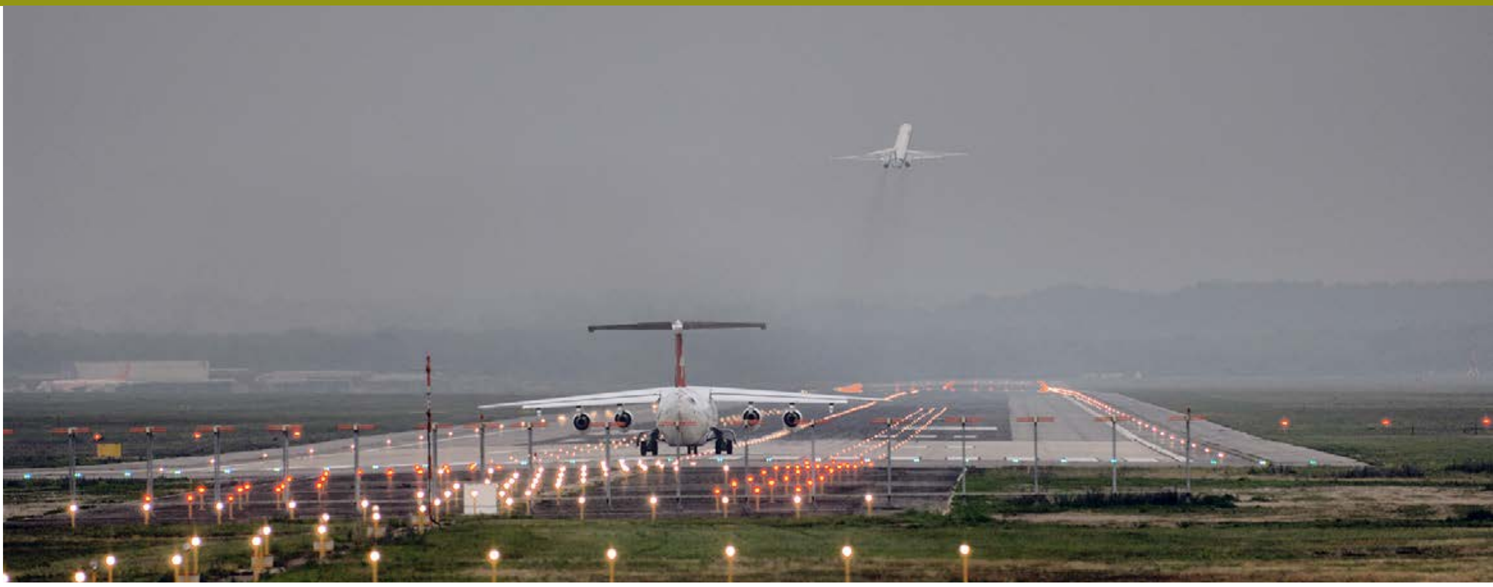
a. Fast screening approaches, facilitating planning and optimisation of resources;

b. Tools for managing compliance with changing regulatory requirements for both security and transport legislation, irrespective of destination and transit airports;

c. Integration capabilities for the optimisation of security and operational efficiency, utilising the latest technologies and best practices with clear and measurable benefits.

PARTNERS	COUNTRY
BMT Group Limited (BMT)	United Kingdom
Swissport International AG (SWP)	Switzerland
Athens International Airport SA (AIA)	Greece
Department for Transport (DfT)	United Kingdom
Conzorzio IB Innovation (IBI)	Italy
Urbanos-Group SGPS SA (URB)	Portugal
Geopost UK Ltd (GEO)	United Kingdom
Fast Freight Marconi SPA (FFM)	Italy
Heavyweight Air Express Ltd (HWE)	United Kingdom
Rapiscan Systems Ltd (RSL)	United Kingdom
MULTIX SA (MLX)	France
Totalforsvarets Forskningsinstitut (FOI)	Sweden
Inlecom Systems Ltd (ILS)	United Kingdom
Conceptivity SARL (CPT)	Switzerland
Mass Spec Analytical Ltd (MSA)	United Kingdom
ENIDE Solutions SL (ENID)	Spain
Commissariat a l'Energie Atomique et aux Energies Alternatives (CEA)	France
MJC2 Ltd (MJC2)	United Kingdom
European Organisation for Security SCRL (EOS)	Belgium
Ingenieria IDOM Internacional SA (IDOM)	Spain
CLMS (UK) Ltd (CLMS)	United Kingdom

GAMMA / Global ATM security management



Information

Grant Agreement N°
312382
Total Cost
€14,837,981.60
EU Contribution
€9,124,760.00
Starting Date
01/09/2013
Duration
48 months

Coordinator

SELEX ES S.P.A. (SELEX)
Air & Vessel Traffic Management Systems
Via Tiburtina, km 12.400
00131 - Rome - Italy
Contact
GIULIANO D'AURIA
Tel: +39 06 41504448
Mobile: +39 335 1629954
Fax: +39 06 41503156
E-mail: giuliano.dauria@selex-es.com
Website: http://www.gamma-project.eu/

Project objectives

The GAMMA project stems from the growing need to address new air traffic management (ATM) threats and vulnerabilities due to the increased reliance on distributed enterprise computing and the automated flow of information across a ground and airborne network. In addition, there is a clear need to establish and implement a comprehensive framework for managing ATM security to minimise the effects of ATM crises brought about by security incidents.

For this purpose GAMMA aims to reach the following main objectives:

» Extend the scope of security risk assessment performed within SESAR (Single European Sky ATM Research) to a more comprehensive system-of-systems level for a global approach to ATM security

» Develop a global ATM security management framework, representing a concrete proposal for the day-to-day operation of ATM security and the management of crises at European level.

» Define the requirements and architecture of an ATM security solution, suitable to support the security management of the global ATM system, in line with the directions and European regulatory baseline identified by the security management framework

» Design and implement representative prototype components of the ATM solution to demonstrate, the functionalities and operations proposed for future European ATM

» Set up a realistic validation exercises, representative of the target ATM solution, through which to validate the feasibility and assess the adequateness of the procedures, technologies, and human resources issues proposed.

Description of the work

To reach these goals, GAMMA will first perform a comprehensive security risk assessment, by taking into account present and emerging set of threats and vulnerabilities affecting the existing ATM system. This analysis will provide the basis for GAMMA to develop a security management framework: a concrete proposal for the day-to-day operation of ATM security. It will also define the requirements and architecture of a security solution which will include the ability to manage incidents and crises spreading throughout the system. The solution will then be tested in exercises using a validation platform to include prototypes and demonstrators developed within the project.

GAMMA will approach the security aspects of the future ATM from an end-to-end perspective, consistent with the full SESAR vision, covering the following domains:

» Airspace security incident management

» Cyber security in ATM information flows

» Communication, navigation and surveillance technologies

» Ground Infrastructure security management

Expected results

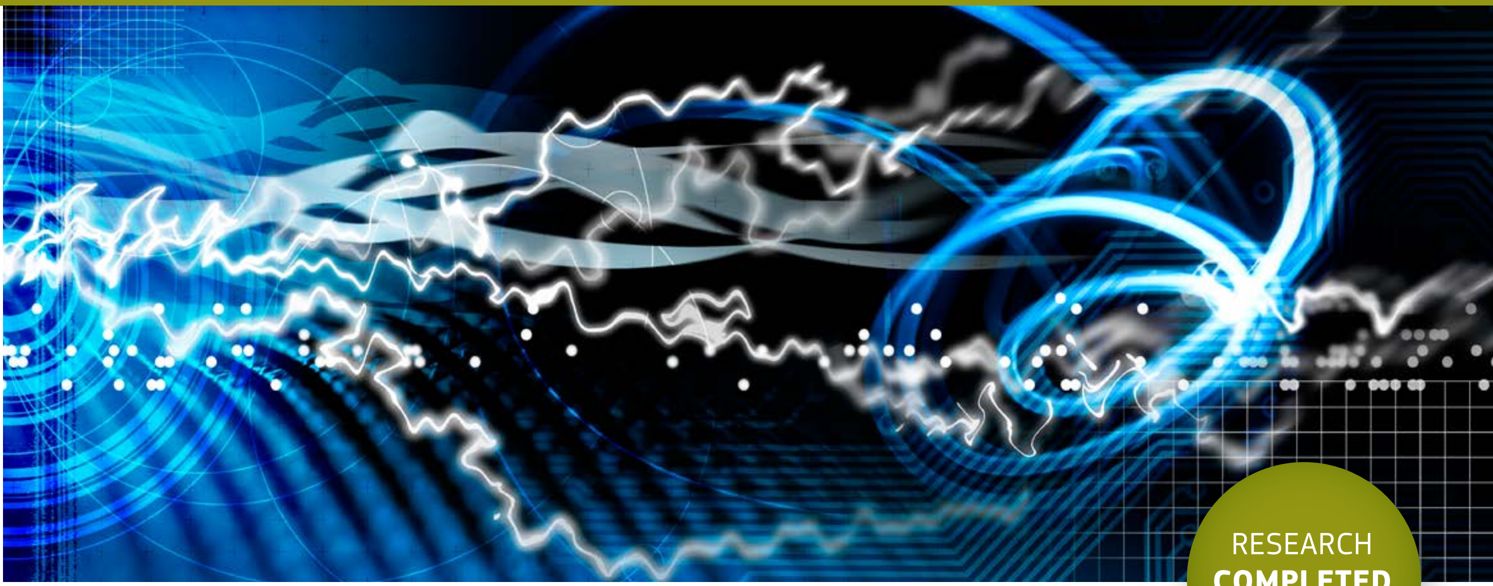
The GAMMA project will produce solutions to emerging air traffic management vulnerabilities, backed up by practical proposals for their implementation.

The initial security risk assessment will result in threat scenarios, security objective reports and associated security controls. This will then be elaborate in a proposed solution covering both operational and technological elements to increase the capability of the ATM system to respond to attacks and manage any crises of the ATM service. The solution developed by GAMMA will be aligned with a proposed institutional framework for ATM security that reflects the interfaces and constraints of stakeholders.

Finally, GAMMA's solutions will be validated via exercises based on prototypes and via validation environments representative of the target architecture.

PARTNERS	COUNTRY
Selex ES S.p.A. (SELEX)	Italy
Airbus Prosky Sas (AIRBUS)	France
Thales Alenia Space España, SA (TASE)	Spain
Boeing Research & Technology Europe S.L.U. (BRTE)	Spain
Enav S.p.A. (ENAV)	Italy
Lancaster University (ULANC)	United Kingdom
Cassidian Sas (CASS)	France
Cassidian Cybersecurity Sas (CYB)	France
Deutsches zentrum fuer Luft – und Raumfahrt EV (DLR)	Germany
RNC Avionics Limited	United Kingdom
Thales Research & Technology (UK) Limited (TRT)	United Kingdom
Società per azioni Esercizi Aeroportuali SEA S.p.A (SEA)	Italy
42 Solutions BV (42S)	The Netherlands
Ingenieria de Sistemas para a Defensa de España SA (ISDEFE)	Spain
Administratia Romana a Serviciilor de Trafic Aerian (ROMATSA)	Romania
Ustav Informatiky, Slovenska Akademia Vied (SAV)	Slovakia
Thales Avionics Sas (THALES)	France
European Aeronautic Defence and Space company EADS France Sas (EADS)	France
CiaoTech Srl (CTECH)	Italy

HIPOW / Protection of Critical Infrastructures against High Power Microwave Threats



RESEARCH **COMPLETED**

Information

Grant Agreement N°
284802
Total Cost
€4,756,371.25
EU Contribution
€3,373578.97
Starting Date
01/06/2012
End Date
31/01/2016

Coordinator

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Protection and Societal Security Division
Instituttveien 20
Po.Box 25
N2027 Kjeller, Norway
Contact
Odd Harry Arnesen
Tel: +47 6380 7671
Mobile: +47 414 08 365
Fax: +47 6380 7509
E-mail:
Odd-harry.arnesen@ffi.no
Website:
www.hipow-project.eu/hipow

Project objectives

1. HIPOW will conduct a threat analysis and risk assessment of the occurrence of severe electromagnetic threats (NNEMP/HPM) and their likely modalities.

2. HIPOW will investigate the influence of NNEMP/HPM pulses on civil objects such as buildings, energy units, transport, banks, communication systems, computer networks, computers and electronic units.

3. HIPOW will evaluate the efficiency of current protection.

4. HIPOW will investigate the feasibility of hardening measures.

5. HIPOW will prepare a NNEMP/HPM detection and diagnostic systems as key tool for a risk management regime (sensor, networking capabilities and data fusion) and a risk management process.

6. HIPOW will build on existing knowledge of NNEMP/HPM protection and develop guidelines and input to standards for protecting civil objects against NNEMP/HPM threats.

Description of the work

The scope of this project lies in three domains:

1. the first is in methodologies for hardening electronic equipment against NNEMP/HPM,

2. the second in the architectures and qualities of contemporary critical infrastructures (CI),

3. and finally the standards, regulations and requirements governing the implementations of protection of CI against NNEMP/HPM attacks. Currently, research on NNEMP/HPM is predominantly carried out within the military sector. The research has not been accessible for the civil sector and CI. Civilian research on the other hand has been primarily dedicated to protecting against relatively benign natural and man-made electromagnetic threats and radiation, and the health effects caused by radiation from civil objects such as mobile phones, medical equipment, etc.

Expected results

The HIPOW project aims to develop a holistic regime for protection of European critical infrastructures against non nuclear high power microwaves (NNEMP/HPM). This includes a suggested risk management process for critical infrastructure organisation and enterprises, developing a NNEMP/HPM detector prototype, and prepare guidelines and recommendations on protection level, and giving advice on how to harden and increase architecture robustness.

PARTNERS	COUNTRY
Forsvarets forskningsinstitutt (FFI)	Norway
Airbus	France
Vojenský technický ústav (VTUVP)	Czech Republic
Instituto de Aplicaciones de las Tecnologías de la Información y de las Comunicaciones Avanzadas (Itaca)	Spain
Grupo Etra (ETRA)	Spain
National Center for Scientiffic Research Demokritos (NCSRD)	Greece
Austrian Institute of Technology (AIT)	Austria
Fraunhofer Institut (FRAUN)	Germany
Net technologies (Net Tech)	Finland
Le centre français de recherche aérospatiale (Onera)	France
Defence Estates Agency (FB)	Norway
Center for Physical Sciences and Technology (CPST)	Lithuania
Qinetiq (Qinetiq)	Great Britain
Defence Logistics Organization (DALO)	Denmark

INFRA / Innovative & Novel First Responders Applications

© Duncan Noakes- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225272
Total Cost
€3,809,464.91
EU Contribution
€2,642,895
Starting Date
01/04/2009
End Date
31/03/2011

Coordinator

ATHENA GS3 SECURITY IMPLEMENTATIONS LTD.
5 Hatzoref St.
Holon 58856
Israel
www.athenaiss.com
Contact
Omer Laviv
Tel: + 972 3 5572462
Fax: + 972 3 5572472
Mobile: + 972 52 8665807
E-mail: olaviv@athenaiss.com
Website: www.infra-fp7.eu

Project objectives

INFRA's research goal was to develop new digital-based personal technologies for integration into a secure emergency management system to support first responders (FRs) involved in critical infrastructure incidents.

This encompassed three broad objectives:

- the creation of an interoperable wireless communications system that functions in difficult FR locales such as subway tunnels or buildings with thick concrete walls;

- the development of a robust indoor site navigation system, based on inertial and wireless sensors, a video annotation system for FR digital devices to generate real-time identification of hazardous materials such as gas leakages, and other sensor-based technologies for the individual first-responder;

- demonstration in live environments to prove the concept's feasibility.

End-users were heavily involved throughout INFRA's various work stages, from requirements-gathering to the final demonstration stages.

Results

The culmination of INFRA's integration work was its final field trial. This was held in January 2011 before a stakeholder audience of FR representatives from across Europe and involved an on-site demonstration of INFRA's entire technology at two locations: inside a tunnel of Madrid's M-30 ring road and a C2 centre located five km away.

The technologies and applications demonstrated in Madrid included:

- a robust ad-hoc mesh topology broadband wireless network for interoperability between standard FR radio sets;

- non-invasive biometric sensors integrated onto a wearable "finger clip" (and an early-prototype ear-clip version) to monitor a first-responder's vital signs such as blood haemoglobin and oxygen levels, heart rate and temperature;

- lightweight optical gas sensors for detecting 02, CO2 and methane levels, and radiation sensors for detecting x-rays, alpha and beta rays, among others;

- a video annotation system to enhance visual communications among FRs and the C2 centre;

- the movements of first responders who were tracked effectively in real-time while in the tunnels;

- a PC-based application, based on client-server architecture, to enable the C2 post to send information requests to first-responders.

According to INFRA's research team, their project achieved all of its technical objectives and, with one exception, tested and demonstrated all of the applications it developed. Moreover, it said the project's novel technology solution could help revolutionise the end-user market since it allows all FR teams, command posts and critical infrastructure control centres to communicate with each other and to transfer digital data at high bit rates, including live video images.

"The field test showed that the main features, though far from complete at the time of the test, nevertheless are functional and deemed very useful by FRs," says INFRA.

PARTNERS	COUNTRY
Athena GS3 Security Implementations Ltd.	Israel
Halevi Dweck & Co. ARTTIC Israel Company Ltd.	Israel
University of Limerick	Ireland
ISDEFE Ingeniería de Sistemas S.A.	Spain
Democritus University of Thrace	Greece
Rinicom	United Kingdom
Everis Spain S.L.	Spain
Hopling Networks B.V.	The Netherlands
Opgal Optronic Industries Ltd.	Israel
Research and Education Laboratory in Information Technologies	Greece
Arttic Israel International Management Services 2009 Ltd (AIL)	Israel

ISTIMES / Integrated system for transport infrastructure surveillance and monitoring by electromagnetic sensing

© TOM ANG – Fotolia.com

Information

Grant Agreement N°
225663
Total Cost
€4,367,950.73
EU Contribution
€3,113,460
Starting Date
01/07/2009
Duration
36 months

Coordinator

TECNOLOGIE PER LE OSSERVAZIONI DELLA TERRA ED I RISCHI NATURALI
c/o CNR-IMAA
C.da S. Loja, Zona Industriale
85050 Tito (PZ)
Italy
Contact
Prof. Vincenzo Cuomo
Tel.: +39 0971 427229/208
Fax: +39 0971 427271
E-mail: tern@imaa.cnr.it
Website: www.istimes.eu

Project objectives

The transportation sector's components are susceptible to the consequences of natural disasters and are attractive as terrorist targets. This is also due to the very high social and economic importance of this sector for the European countries. On the other hand, the terrorist events of the last years have pointed out that achieving clear and concise situational awareness is a key factor in the crisis management. This entails accurate monitoring as well as the possibility of obtaining quasi real-time information on the scenario of crises.

In this framework, the ISTIMES project aims at designing, assessing and promoting an ICT-based system, exploiting distributed and local sensors, for non-destructive electromagnetic monitoring of the critical transport infrastructures. The outcomes of the monitoring system are in terms of detailed real time information and images of the infrastructure status to be used to provide support to the decision of emergency and disaster stakeholders.

Description of the work

The ISTIMES project aims at designing a prototype electromagnetic sensing monitoring and surveillance system to improve safety and security of the transportation infrastructures. The system will use and integrate heterogeneous, state-of-the-art electromagnetic sensors, enabling a self-organizing, self-healing, ad-hoc networking of terrestrial in situ sensors, supported by specific airborne and satellite measurements. The effectiveness of the system will be tested at two challenging test beds in Switzerland and Italy.

The project activities of ISTIMES have been broken down into five activities:

» ACTIVITY 1 will cover the definition of user requirements of the system for the electromagnetic diagnosis and monitoring of strategic infrastructures. This is a key activity for the acceptance of the usefulness of the system from the end user's point of view;

» ACTIVITY 2 will deal with the development of the ISTIMES e-infrastructure organized in three sub-infrastructures: infrastructure for real time and interactive access to the information by end-users; infrastructure for enabling remote use of and control of instrumentation and processing of measurements; wireless network services for sensor communication;

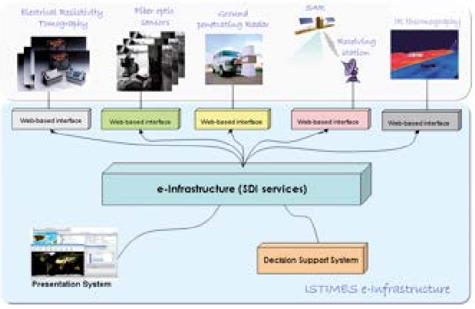
» ACTIVITY 3 will deal with the exploitation, improvement, and integration of processing approaches and measurement strategies for non invasive monitoring of the structure at different temporal and spatial scales. Several electromagnetic sensing techniques will be exploited and their performance analysis will be performed in controlled conditions at state-of-the-art and innovative test sites;

» ACTIVITY 4 will deal with the implementation of the system and demonstration activities at two test beds such as a highway-bridge in Switzerland and railway and highway infrastructures in Italy;

» ACTIVITY 5 will deal with the dissemination, technological transfer and use-exploitation of the project results.

Expected results

- A prototype of an electromagnetic sensing (ES) monitoring and surveillance system based on an ad-hoc networking of in situ sensors and airborne/satellite data;
- 4D tomographic infrastructure monitoring thanks to the exploitation and integration of the ES techniques;
- Validation of ES techniques through experiments at two test sites;
- Demonstration of the effectiveness of the system at two challenging test beds;
- Dissemination of the ISTIMES approach and outcomes to public institutions and private companies.



© Istimes

PARTNERS	COUNTRY
Tecnologie per le Osservazioni della Terra ed i Rischi Naturali (TeRN)	Italy
Elsag Datamat (ED)	Italy
Dipartimento di Protezione Civile (DPC)	Italy
Eidgenoessische Materialpruefungs- und Forschungsanstalt (EMPA)	Switzerland
Laboratoire Central des Ponts et Chaussées (LCPC)	France
Lund University (ULUND)	Sweden
Tel Aviv University (TAU)	Israel
Territorial Data Elaboration SRL (TDE)	Romania
Norsk Elektro Optikk (NEO)	Norway
Telespazio S.p.A. (TPZ)	Italy

L4S / Learning for security project

© fotografiche.eu - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225634
Total Cost
€3,471,413.41
EU Contribution
€2,415,768
Starting Date
01/07/2009
End date
31/07/2011

Coordinator

DELOITTE BUSINESS SOLUTIONS ANONYMI ETAIREIA SYMVOULON EPICHEIRISEON
c/o CNR-IMAA
C.da S. Loja, Zona Industriale
85050 Tito (PZ)
Italy
Contact
Christos Konstantinou
E-mail: ckonstantinou@deloitte.gr
Website:
www.L4S-project.info

Project objectives

The L4S project sought to develop an easily deployable life-long learning service to improve the crisis management skills and competencies of security personnel (notably top management). L4S simulation-based crisis management exercises focused particularly on air and sea transport disaster scenarios.

The project's target audience for improved crisis management skills comprised European corporate personnel, decision-makers and academic learners, with an eye to strengthening the resilience of private and public organsiations in Europe. Three types of crisis management-relevant competencies were addressed: cognitive abilities, affective and normative aspects of learning, and the ability to perform an action.

Results

The project designed and developed the "L4S learning experiences service" consisting of advanced simulation games and learning/networking applications. The L4S portfolio includes the following air and sea transport crisis management simulation exercises:

» "IMPACT: The Crisis Readiness Online Simulation Experience";

» "RECKON&CHOOSE! Air Simulation";

» "CRISIS TEAM".

Apart from simulation games, the L4S portfolio also contains a WEB 2.0 advanced networking and sharing tool named "CRISIS TUBE Leadership Learning Network", as well as a supportive online workshop tool known as "OWL4S".

The individual exploitation plans of the partners explored the potential use of three different types of L4S applications:

» *Internal:* organisations that integrate the L4S applications portfolio in their internal executive training programs, offering employees and executives the opportunity to take part in this type of learning experience;

» *External:* commercial entities that distribute the L4S applications portfolio to their customers in various industries, with possibilities for learning experiences to be bundled with existing business products or services;

» *Academic:* educational and academic institutions that integrate L4S training applications in their curricula. The L4S portfolio could also serve as basis for executive and vocational training.

The consortium believes that L4S simulation games and applications can provide impact and visibility, along with the generation of a strong stream of revenue for those organisations choosing to implement them. The long-term strategy is to set up an efficient Europe-wide B2B Channel for the diffusion of similar game-based learning experiences.

PARTNERS	COUNTRY
Deloitte Business Solutions Anonymi Etairia Symvoulon Epicheiriseon	Greece
Oesterreichische Studiengesellschaft Fuer Kybernetik	Austria
Alphalabs SARL	France
Universitaet Der Bundeswehr Muenchen	Germany
Athens Laboratory of Business Administration	Greece
Universita Cattolica Del Sacro Cuore	Italy
FVA SAS	Italy
Athens International airport S.A.	Greece
Creurers del port de Barcelona SA	Spain
Frequentis AG	Austria
Akad Wissenschaftliche Hochschule Lahr GMBH	Germany

NI2S3 / Net-centric information and integration services for security systems

© Aaron Kohr - Fotolia.com

Information

Grant Agreement N°
225488
Total Cost
€4,325,739.94
EU Contribution
€2,711,640
Starting Date
01/07/2009
End Date
30/09/2011

Coordinator

VITROCISET S.P.A.
Contact
Walter Matta
Tel: +39 06 88202567
Mobile: +39 335 7716488
Fax: +39 06 8820 2288
E-mail: w.matta@vitrociset.it
Website:
http://ni2s3-project.eu/

Project objectives

The main objective of NI2S3 was to research and implement a reference methodology for developing security systems based on networked or electronic information and integration services for critical infrastructure protection (CIP).

A key goal was to integrate information from numerous heterogeneous sensors or sources, in order to build up and improve situational awareness around critical infrastructures.

Results

The basis of NI2S3 was a gap analysis of situational awareness capacities around critical infrastructure protection in Europe.

The goal of this analysis was to identity where a network-centric “information space” could be of use to support CIP decision makers. This space was conceptualised as a layer of interoperable ICT that can support the input of dedicated devices, public information and services to optimise resource management. Such a space can provide superior information on events and conditions surrounding infrastructures in an emergency, or for day-to-day management.

Scenarios and locations considered for this concept included a new command and control (C2) architecture to support Polish police in the city of Kracow, an information service on Kracow’s public highways and an information service for the A22 highway in northern Italy.

These scenarios were used to assess potential “spoiler” inputs to an open information system – including such factors as hostile eavesdropping on information traffic, data interception/alteration for malicious purposes and the mass flooding of the system with “spam” or false data or to create denial of service via voluminous spam. False safes such as sensor kill-switches and data encryption were proposed to handle these threats.

The final operational concept has now been submitted for stakeholder examination.

PARTNERS	COUNTRY
Vitrociset S.p.A.(VCS)	Italy
Università degli Studi di Firenze (UNIFI)	Italy
HW Communications Limited (HWC)	United Kingdom
AALBORG Universitet (AAU)	Denmark
AGH University of Science and Technology (AGH)	Poland
Comarch S.A. (COMARCH)	Poland

PANDHUB / Prevention and Management of High Threat Pathogen Incidents in Transport Hubs

Information

Grant Agreement N°
607433
Total Cost
€3,986,784
EU Contribution
€3,142,004
Starting Date
01/11/2014
Duration
36 months

Coordinator

TEKNOLOGIAN TUTKIMUSKESKUS VTT OY (VTT)
Efficient machines and vehicles
Tekniikankatu 1
PO Box 1300
FI-33101 Tampere, Finland
Contact
Ilpo Kulmala
Tel.: +358 207223263
Mobile: +358 207223263
Fax: +358 207223499
E-mail: ilpo.kulmala@vtt.fi
Website:
www.pandhub-fp7-security.eu

Project objectives

PANDHUB will create an integrated toolbox to aid transport operators and relevant actors to develop their pandemic and dangerous pathogen preparedness and response plans. The project is intended to cover the extraordinary aspects specific to serious natural or man-made pathogen threats in the transport environment. This will be achieved by providing accurate, reliable and validated information for the incident threat assessment, preparedness, and response phases.

Description of the work

The management of large scale incidents may be divided into the following phases: threat assessment, prevention, preparedness, and response and recovery. PANDHUB will collect and develop tools for each of these phases.

A special need for new developments is required, especially, in respect of epidemiological surveillance and contact tracing. Other research activities include threat assessment in transport hubs, communication and decontamination tools, and guidelines for both the handling of pandemics and for the protection of people and infrastructure.

The developed tools will be tested through workshops and field exercises. The feedback from these experiments will be used for validation and further development of the tools.

Expected results

The resulting integrated toolbox will include:

- » A threat and vulnerability assessment toolbox
- » A preparedness tool set
- » A response tool set
- » An incident response coordination, cooperation, and communications tool set.

The toolbox will also include modelling components to simulate the spread of diseases and to evaluate the effectiveness of countermeasures.

With the aid of the developed tools PANDHUB will enhance the protection of transport hubs against the threat of pandemics and thus assist in the creation of safer travel environments.

PARTNERS	COUNTRY
Teknologian tutkimuskeskus VTT Oy (VTT)	Finland
Assistance Publique – Hôpitaux de Paris (ASSISTANCE PUBLIQUE)	France
Department of Health (DH)	United Kingdom
Institut de Médecine et de Physiologie Spatiales (MEDES)	France
Itä-Suomen Yliopisto (UEF)	Finland
The University of Nottingham (UNOTT)	United Kingdom

PANDORA / Advanced training environment for crisis scenarios

© Evan Luthye - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225387
Total Cost
€3,997,166.21
EU Contribution
€2,930,000
Starting Date
01/01/2010
End Date
31/03/2012

Coordinator

UNIVERSITY OF GREENWICH
Old Royal Naval College,
Park Row, Greenwich
UNITED KINGDOM
Contact
Reginald DALY
Tel: +44 02083319685
Fax: +44 02083318665
Website: http://PANDORA-project.eu/

Project objectives

PANDORA is a crisis management project developing a training toolset and environment, which aims to bridge the gap between tabletop exercises and real world simulation exercises. The project proposes a global approach to crises management, providing a near-real training environment at an affordable cost.

The project will create an environment that can provide appropriate metrics on the performance of a crisis manager actively engaged in the management of a crisis, with the environment providing:

» A realistic and complete scenario with near real-time action, coherent with that expected in a real-world situation;

» Realistic emotional status, through affective inputs and stress factors;

» The potential to include different crisis managers belonging to different sectors.

PANDORA offers a focus on the emotional status of the crisis manager because such knowledge, in all phases of emergency management, is critical to the development of effective emergency policies, plans and training programs.

Description of the work

To achieve the aims of the PANDORA project, the workload has been broken down into 9 work packages:

» *WP1:* User Requirements Analysis and design of PANDORA functional specifications – will provide a definition of both data and workflows needed to specify the proposed system and to clearly identify the processes that are the basis of the system services;

» *WP2:* Behaviour simulation and modelling - split into 5 tasks: the first two consolidate the basic preconditions for the behavioural planner, the third designs the general architecture of the planner, the remaining two provide proactive reasoning services to the planner;

» *WP3:* Crisis simulation and modelling - focused on three main modules: (1) the crisis knowledge base, (2) the crisis planner that generates the conceptual high level network of events that constitutes the plot for the scenario, and (3) the crisis modeller that tracks the evolution in real time of the scenario;

» *WP4:* Environment and Emotion Simulation Engine – seeks to integrate emotional human factors within training programs for crisis managers, taking into account several research topics:

- Relevant human factors in crisis decision-making;
- Neuro-physiological testing and measures;
- Personalised and flexible training strategies.

» *WP5:* Environment design and building – seeks to authentically recreate the dynamic elements of the entire disaster environment, i.e. emulating a complete crisis room with realistic visuals and audio to create an immersive, chaotic and stressful environment;

- *WP6:* Development, integration and testing – will deliver the PANDORA software product that can be considered as a system composed of software subsystems/components implemented in different environments;
- *WP7:* Training testing, evaluation and assessment – will support the development of a robust evaluation methodology that complements the work done to build the PANDORA advanced training environment;
- *WP8:* Dissemination and exploitation;
- *WP9:* Project management.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
University of Greenwich (UoG)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR-ISTC)	Italy
Società Consortile a Responsabilità Limitata (CEFRIEL)	Italy
Razvoj programske opreme in svetovanje d.o.o. (XLAB)	Slovenia
Fondazione Ugo Bordoni (FUB)	Italy
ORT FRANCE (ORT)	France
University of East London (UEL)	United Kingdom
Business Flow Consulting (BFC)	France
Emergency Planning College (EPC)	United Kingdom

PROGRESS / Protection and Resilience Of Ground based infRastructures for European Space Systems

Information

Grant Agreement N°
607679
Total Cost
€4,711,595.20
EU Contribution
€3,337,014.00
Starting Date
01/05/2014
Duration
36 months

Coordinator

COMMISSARIAT À L'ÉNERGIE ATOMIQUE ET AUX ÉNERGIES ALTERNATIVES (CEA)
CEA GRAMAT
ROUTE DE REILHAC,
46500 GRAMAT, FRANCE
Contact
Nicolas Ribière-Tharaud
Tel.: +33 5 65 10 55 66
E-mail:
Nicolas.RIBIERE-THARAUD@CEA.FR
Website:
www.progress-satellite.eu/

Project objectives

PROGRESS has 7 main objectives:

1. Development of risk assessment methodology and tool to assess threats on generic Global Navigation Satellite Systems (GNSS) ground based infrastructure and assets operating space systems and their secure communication links to satellites and a prioritization of the threats for which detection, protection, and mitigation solutions should be developed.

2. Development of detection and location solutions for: cyber attacks (e.g. DoS attacks and spoofing), RF interferences (jamming and spoofing), and physical attacks (explosive and high power microwaves. These detectors will be gathered in an Integrated Ground Station Security Monitoring System (IGSSMS).

3. Development of threat protection and mitigation solutions for the cyber, RF interferences and physical attacks: guidelines, architecture solutions, tools and methods, and procedures to be implemented once an attack(s) is identified.

4. Development of a Security Control Centre (SCC) to analyse the impact of detected threats and to propose mitigation procedures, including system reconfiguration.

5. Development and integration of a prototype Security Management Solution (SMS) to prove the PROGRESS innovative security concepts, including the IGSSMS and SCC.

6. Testing and evaluation of the prototype SMS.

7. Further development of strategies to exploit the results of the project.

Description of the work

PROGRESS focuses on improving the security and resilience of GNSS.

At the beginning of the project, a generic GNSS system and its associated augmentation system was designed and assessed with regards to vulnerability from intentional malicious threats. The focus was threats which are generally considered to have a low risk of occurrence but potentially very large impacts and that have the potential to increase in the coming years. The resulting prioritisation of threats and scenarios is being used as input to develop a prototype Security Management Solution (SMS).

The SMS will be a centralised solution able to automatically detect malicious actions with a built-in reconfiguration capability to ensure the overall system Quality of Service. The SMS will be composed of an Integrated Ground Station Security Monitoring System (IGSSMS) and a Security Control Centre (SCC). The IGSSMS will be an innovative monitoring solution for the detection of specific malicious types of attacks. The Security Control Centre will analyse the impact of the reported disturbances to the system performance and Quality of Service (QoS) and will propose mitigation strategies, including automatic system reconfiguration.

Expected results

Core prototype results:

» Risk assessment methodology

A holistic methodology enabling assessment of threat scenarios on GNSS, including the potential impact on society.

» Security Management Solution (SMS)

Centralised solution able to automatically detect attacks, analyse their impact, and propose mitigation actions, including reconfiguration to ensure overall GNSS quality of service. The SMS will consist of:

» Integrated Ground Station Security Monitoring System (IGSSMS) with integrated detectors for cyber, RF and physical attacks.

» Security Control Center (SCC) to analyse the impact of events reported by IGSSMS and to trigger protection and/or mitigation procedures, including recommendations for system reconfiguration.

» On Board Security Unit (OBSU)

Telemetry, Tracking & Control (TT&C) encryption solution for communication between satellites and ground stations.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Crabbe Consulting Ltd (CCLD)	United Kingdom
DLR Gesellschaft für Raumfahrtanwendungen GfR mbH (DLR GfR)	Germany
Thales Alenia Space France (TASF)	France
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V. (Fraunhofer EMI)	Germany
Thales Alenia Space Italia SPA (TASI)	Italy
Decisio BV (DECISIO)	The Netherlands
QASCOM Srl (QASCOM)	Italy
Securiton GmbH (SECURITON)	Germany
Thales Alenia Space España SA (TASE)	Spain
Univerza v Ljubljani (UL)	Slovenia

PROTECTRAIL / The Railway-Industry Partnership for Integrated Security of Rail Transport

© PROTECTRAIL

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242270
Total Cost
€21,632,880.80
EU Contribution
€13,115,064
Starting Date
01/09/2010
End Date
30/06/2014

Coordinator

ANSALDO STS S.P.A.
Via P. Mantovani 3-5
16151 Genova
Italy
Contact
Mr. Vito Siciliano
Tel.: +39 010 6552976
Fax: +39 010 6552006
Mobile: +39 3489895875
E-mail: Vito.Siciliano.
Prof110@ansaldo-sts.com

Project objectives

The objective to provide a viable integrated set of security solutions, by considering the extent of the assets involved, the nature of the threats, the amount of requirements and the constraints. The integration will follow an innovative way and will extend the scope of the project beyond the mission addressed by the call.

The PROTECTRAIL will develop mission oriented vs. asset-specific solutions and will make them interoperable by designing a modular architectural framework where each solution can be "plugged". This will provide the basis for a streamlined process of federation, integration and interoperability.

The project will ensure that appropriate solutions and innovations are favoured over isolated questions and solutions, and will represent a comprehensive and scalable answer to rail security.

The dissemination process will initiate a cooperation framework with the National and EU authorities and the standardisation bodies, in view of proposals for recommendations to be adopted.

Description of the work

PROTECTRAIL designed an interoperability framework built on a system-of-systems approach into which asset-specific and interoperable security solutions can be "plugged". This gives operators and infrastructure managers the possibility to adapt their security systems to changing security needs with minimal non-recurring costs. This framework consists of a set of rules and standards which facilitate the integration and communication amongst various security technologies. It is based on three concepts, namely that:

1. interoperability is improved through standardisation

2. re-use of existing and relevant international standards are preferred

3. simplicity is the key to long-term adoption.

Results

PROTECTRAIL tested this interoperability framework during field demonstrations at the main test site in Zmigrod, Poland and at satellite sites in Villecresnes,France and Palermo,Italy). These tests concentrated on four priority facets: an event-driven Service-Oriented Architecture (SOA), network communications, video management, and security technologies. PROTECTRAIL has met the challenges of both combining a large variety of technological and procedural security solutions, and reinforcing the strength of these solutions in a global and coherent system.

The methodology for the integration of security technologies in PROTECTRAIL has worked and has shown to be efficient, scalable and able to evolve with time. This is due to its simplicity, non-proprietary nature and standardisation. The integration of security technologies in the railway sector has thus been confirmed to be a complex but achievable goal, facing a broad spectrum of threats, from low-probability-high-impact events (e.g. terrorist attack) to high-probability-low-impact events (e.g. copper theft).

PARTNERS	COUNTRY
Ansaldo STS S.p.A.	Italy
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Elsag Datamat S.p.A.	Italy
Union Internationale Des Chemins De Fer	France
Selex Sistemi Integrati S.p.A.	Italy
Bombardier Transportation GMBH	Germany
Alstom Transport SA	France
Thales Security Solutions & Services SAS	France
Sarad GmbH	Germany
UNIFE – The European Rail Industry	Belgium
Sagem Sécurité SA	France
Ductis GmbH	Germany
Železničná spoločnosť Slovensko a.s.	Slovakia
Joint Stock Company Lithuanian Railways	Lithuania
ItalCertifer S.c.p.a.	Italy
PKP Polskie Linie Kolejowe SA	Poland
D'Appolonia S.p.A.	Italy
Elbit Systems Ltd.	Israel
Facultés Universitaires Notre-Dame de la Paix	Belgium
EPPRA	France
Kingston University Higher Education Corporation	United Kingdom
SODERN	France
Smiths Heimann S.A.S.	France
Rail Cargo Austria	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Institut Franco-Allemand de Recherches de Saint-Louis	France
Turkish State Railways	Turkey
MER MEC S.p.A.	Italy
Société Nationale des Chemins de Fer	France

SCOUT / Multitech SeCurity system for intercOnnected space control groUnd staTions

Information

Grant Agreement N°
607019
Total Cost
€3,491,731.80
EU Contribution
€2,382,677.70
Starting Date
01/11/2014
Duration
36 months

Coordinator

CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT)
Radar and Surveillance Systems National Laboratory (RaSS)
Galleria G.B. Gerace N° 18,
56124 - Pisa, Italy
Contact
Fabrizio Berizzi
Tel.: +39 050 3820 523
Mobile: +39 335 6813113
Fax: +39 050 3820571
E-mail: fabrizio.berizzi@cnit.it
Website:
www.scout-project.eu

Project objectives

The main goal of SCOUT is to study, design and assess a security system based on multiple technologies to protect space control ground stations and the satellite links against physical and cyber attacks. It is also important to activate automatic restoration and intelligent reconfiguration mechanisms in case of failure concerning the ground stations networks and the satellite links.

Description of the work

The SCOUT system is composed of three different subsystems:

1. A scalable distributed multisensor network for protection against physical attacks (SENSNET subsystem), which is composed of low impact sensor, namely passive sensors (passive radar, infrared camera, radiometric radar) and low emission radars such as noise radar-based sensors or NRBS).

2. A distributed telecommunications network sensing system for the detection and protection against cyber attacks of telecommunication links (CYBERSENS subsystem), composed of several network probes (monitoring devices located at every ground stations), host probes (lightweight software sensing agents residing in the actual ground station machines), a honeynet (a decoy network used to detect and track cyber attacks), and a central engine which coordinates the entire infrastructure.

3. A management network system for automatic restoration and intelligence reconfiguration of the space control ground station network (RECOVER subsystem), designed in accordance to the distributed Smart Sensor Network paradigm where the reconfiguration and control is governed by distributed logic.

The first two subsystems (SENSNET and CYBERSENS) allow for the acquisition of information about potential attacks to the ground station and/or possible damages of attacks once inflicted. This data is processed by a centralised main control unit (MCU) to gain a situation awareness picture, which is used to assess the degree of alert.

The SENSET and CYBERSENS subsystems are controlled to focus their resources on potential threats. According to the result of the assessment, the RECOVER system is activated.

Therefore, the main tasks of the MCU are:

1. A data processing

2. A decision making support

3. A subsystem control, with graphical user interface included

Two risk tools have been developed to identify the vulnerabilities of the ground station against physical and cyber attacks and to drive the design and functionalities of subsystems and MCU. These tools are used for a static analysis of the ground station vulnerabilities to be used in the SCOUT design phase, but they are also employed dynamically for the SCOUT system functioning.

Expected results

The capability of the SCOUT system will be proved by development of a proof-of-concept demonstrator.

PARTNERS	COUNTRY
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Italy
Vitrociset spa	Italy
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V.	Germany
Metasensing BV	The Netherlands
Politechnika Warszawska (WUT)	Poland
A. Usikov institue of Radiophysics and Eletronics, National Academy of Sciences of Ukraine (IRE NASU)	Ukraine
Universidad de Alcala (UAH)	Spain
Oesia Networks srl	Spain
Agenzia Spaziale Italiana (ASI)	Italy

SECRET / SECurity of Railways against Electromagnetic aTtacks

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285136
Total Cost
€4,256,416.80
EU Contribution
€3,059,433.00
Starting Date
01/08/2012
End Date
30/11/2015

Coordinator

INSTITUT FRANCAIS DES SCIENCES ET TECHNOLOGIES DES TRANSPORTS, DE L'AMENAGEMENT ET DES RESEAUX (IFSTTAR)
IFSTTAR-Components and Systems
20, rue Élisée Reclus
BP 70317
F-59666 Villeneuve d'Ascq Cedex
Contact
DENIAU Virginie
Tel.: +33 3 20 43 89 91
Mobile: +33 6 07133345
E-mail: Virginie.deniau@ifsttar.fr
Website: www.secret-project.eu

Project objectives

SECRET addresses the protection of railway infrastructure against electromagnetic (EM) attacks. Railway infrastructure is an attractive target for such attacks because of its familiarity and ease of access, with extended economic and security consequences.

SECRET's objectives are to:

» identify the vulnerability points at different levels (from the electronic to the systemic vision)

» identify EM attack scenarios and risk assessment (service degradation, potential accidents, economic impacts...)

» identify public equipment which can be used to generate EM attacks

» develop protection rules to strengthen the infrastructure (at electronic, architecture and systemic levels)

» develop EM attack detection devices and processes

» develop resilient architecture to adequately react in case of EM attack detection

» extract recommendations to ensure resiliency and contribute to standards

Results

The exploitable results were the recommendations issued by the project:

» A SECRET architecture for resilient communication under EM attacks

» SECRET's technical recommendations on preventive and recovery measures as well as a suitable methodology to evaluate and mitigate EM attacks in the railway context of:

- standardisation,
- engineering guidelines
- operational

Some of the project's information is very sensitive, meaning that publication of the results must take this into account. The main sensitive information is related to work-packages 1 and 2 (vulnerability of railway management system, devices available that can be used to generate EM attacks, analysis of susceptibilities of communication or control-command devices of the infrastructure against EM signal attacks) .

PARTNERS	COUNTRY
ALSTOM BELGIUM SA (ALSTOM BELGIUM)	Belgium
+ ALSTOM TRANSPORT France (ALSTOM Transport - 3rd Party)	France
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V (Fraunhofer)	Germany
POLITECNICO DI TORINO (POLITO)	Italy
SOCIETE NATIONALE DES CHEMINS DE FER FRANCAIS (SNCF)	France
TRIALOG (Trialog)	France
UNION INTERNATIONALE DES CHEMINS DE FER – (UIC)	France
UNIVERSITE DE LIEGE (ULG)	Belgium
UNIVERSIDAD DEL PAIS VASCO EHU UPV (EHU)	Spain
ZANASI ALESSANDRO SRL & PARTNERS (Zanasi & Partners)	Italy

SECTRONIC / Security system for maritime infrastructure, ports and coastal zones

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218245
Total Cost
€6,948,326.42
EU Contribution
€4,496,106.41
Starting Date
01/02/2008
End Date
31/01/2012

Coordinator

QUEEN MARY,
UNIVERSITY OF LONDON
MARINE & REMOTE
SENSING SOLUTIONS LTD
Suite 100
Saint-James Place 11
UK – SW1A 1NP London
United Kingdom
Contact
Dr. Sverre Dokken
Tel: +44 2078 712 800
E-mail:
sdokken@marss.co.uk
Website: www.sectronic.eu

Project objectives

The SECTRONIC initiative addresses observation and protection of critical maritime infrastructures: Passenger and goods transport, Energy supply, and Port infrastructures.

All accessible means of observation (offshore, onshore, air, space) of those infrastructures are networked via an onshore control center.

The end-users themselves or permitted third-parties can access a composite of infrastructure observations in real-time. The end-users will be able to shield the infrastructure by protective means in security-related situations.

The proposed system is a 24h small area surveillance system that is designed to be used on any ship, platform, container/oil/gas terminal or port and harbour infrastructure.

The initiative is an end-users driven R&D activity.The overall objective of the SECTRONIC research project is to develop an integrated system for the ultimate security of maritime infrastructures covering ports, passenger transport and energy supply against being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour.

The project aims to develop an integrated security system that:

» Accurately observes, characterizes and tracks any object of significance, 360 degrees around an infrastructure, 24 h a day in all weather conditions by means of:

- Near range equipment
- Far range equipment

» Communicates security information of significance to the infrastructure authorities (sea masters, operation control managers, etc.) and to selected authorised third parties of importance for the overall security situation (port authorities, coast guards, etc.) in real time.

» Aggregates, reports and displays any security-related information of significance in an intuitively understandable way. Reliably raises alarms in identified situations.

» Enables response procedures and actions to be undertaken in situations that require effective use of protective measures.

» Demonstrates system effectiveness in real maritime infrastructures.

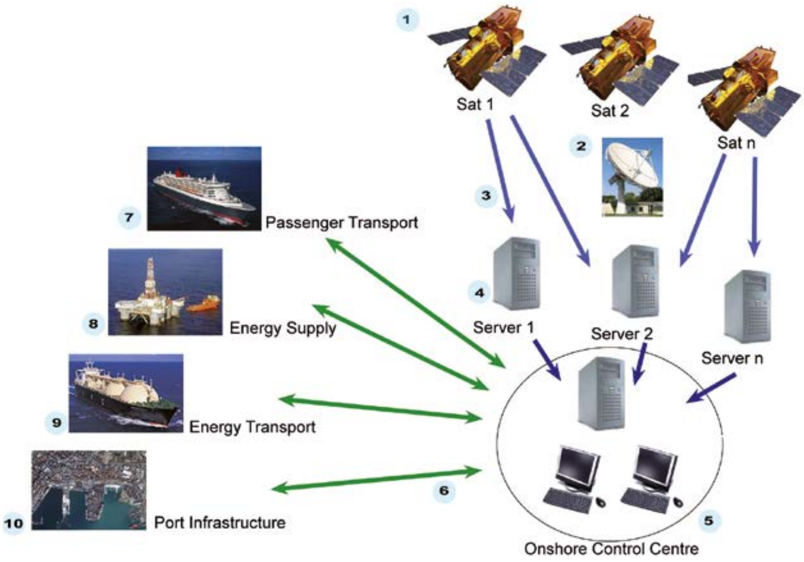
Results

The project aimed to develop an integrated system for the security of maritime facilities: ports, passenger transport and energy supply. Project partners combined various observation systems (radar, sonar and Earth Observation (EO) satellites) to develop an early warning system that can be installed on a ship's bridge or in port control rooms.

This early warning system tracks and characterises objects of significance in a 360 degree radius around the infrastructure. Any identified threats are then communicated to the managers of the infrastructure and relevant authorities. The SECTRONIC system also facilitates responses to the identified threat(s).

As part of this work, the project analysed performance gaps in existing monitoring facilities, based on user-defined scenarios, and recommended new sensors and algorithms. SECTRONIC also assessed current security alert reporting and operational performance practices. In addition, to make the system as user friendly as possible and to minimise response time, the project team identified optimal ways to integrate security information into the graphical user interface.

SECTRONIC's findings will help facility managers and emergency services to keep Europe's marine infrastructures safe from harm by identifying risks and responding to them effectively.



© Sectronic

PARTNERS	COUNTRY
Queen Mary, University of London Marine & Remote Sensing Solutions Ltd	United Kingdom
Uniresearch B.V.	The Netherlands
Det Norske Veritas AS	Norway
Norwegian Defence Research Establishment	Norway
Chalmers University of Technology	Sweden
Advanced Computer Systems ACS S.p.A.	Italy
Nato Undersea Research Centre	Italy
Carnival Corporation.	United Kingdom
BW Offshore AS	Norway
BW Gas ASA	Norway
Havenbedrijf Rotterdam N.V.	The Netherlands
Autorità Portuale della Spezia	Italy

SEGRID / Security for smart Electricity GRIDs

Information

Grant Agreement N°
607109
Total Cost
€4,541,551
EU Contribution
€3,402,022
Starting Date
01/10/2014
Duration
36 months

Coordinator

ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO (TNO)
Cybersecurity & robustness
Anna van Buerenplein 1
Postbus 96800
2509 JE - The Hague
The Netherlands
Contact
Reinder Wolthuis
Tel.: +31 888667787
Mobile: +31 6 51913379
Fax: +31 8886 67757
E-mail:
reinder.wolthuis@tno.nl
Website: www.segrid.eu

Project objectives

SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks. It will deliver a major contribution to the protection of future smart grids against cyber-attacks by:

- Identifying threats and potential future cyber-attack pathways for the SEGRID use cases;
- Determining the gaps across available security standards, methods and measures for smart grids in order to derive which additional security methods and measures are required for the SEGRID use cases;
- Developing new security methods and measures for privacy, communication and system security in smart grids;
- Building up a realistic test environment to test and verify new security methods and measures;
- Evaluating and improving current risk management methodologies to make them optimally suited to address the key risk factors of smart grids of 2020;
- Feeding SEGRID's results into European and global standardization bodies, industry groups and smart grid suppliers.

Description of the work

SEGRID looks upon the smart grid as a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the smart grid as a whole. It has defined five use cases based on a gradually evolving system concept. These reflect important steps of the smart grid developments for the coming years, as well as the addition of new functionality and components that will introduce new vulnerabilities and widen cyber-attack surface.

The five SEGRID use cases are:

1. Smart meter used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.

First, we will design a reference architecture, specify the use cases and formulate privacy and security goals for the SEGRID use cases. Next we will evaluate risk assessment (RA) methodologies for smart grids and perform this on SEGRID use cases. The goal of these risk assessments is twofold:

- identify current and future threats, vulnerabilities and risks of cyber-attacks against smart grids;
- identify shortcomings in RA methodologies to develop enhancements to improve applicability of these RA methodologies for future smart grids.

The identified threats, vulnerabilities and risks will be used to perform a gap analysis where the gaps between required and currently available security technologies for smart grids will be identified. SEGRID will develop novel security solutions to address some of these gaps, and develop a roadmap to guide future research in this field. SEGRID is developing novel security solutions in the areas of:

- System & platform security,
- Communication protocols security,
- Resilient communications infrastructure, and
- Privacy by design.

One of the unique features of SEGRID is the design and implementation of a "Security Integration Test Environment" (SITE). Combining state of the art test facilities at several locations in Europe, SEGRID will test the developed vulnerability assessment tools and security solutions in testing environments that simulate future smart grid infrastructures.

Last but not least, SEGRID will identify improvements with respect to smart grid security and privacy in policies and regulations, and perform a cost assessment for the application of developed novel security solutions.

Expected results

SEGRID will provide essential insight to identify, assess and address the threats, vulnerabilities and risks of cyber-attacks in future smart grids.

It will deliver tools to analyse threats, risks and vulnerabilities in smart grids, and a set of novel security technologies to improve the security, privacy and resilience of the future smart grid.

PARTNERS	COUNTRY
Organisatie voor toegepast natuurwetenschappelijk onderzoek TNO (TNO)	The Netherlands
Swedish Institute of Computer Science (SICS)	Sweden
Kungliga Tekniska högskolan (KTH)	Sweden
Instituto Consultivo para el Desarrollo INCODE (IND)	Spain
European Network for Cyber Security (ENCS)	The Netherlands
Liander NV (ALL)	The Netherlands
ABB AS corporate research (ABB)	Norway
Foundation of the Faculty of Sciences of Lisbon University (FFCUL)	Portugal
Energias de Portugal (EDP)	Portugal
ZIV Metering Solutions S.L. (ZIV)	Spain

SERON / Security of road transport networks

© Frog 974- Fotolia.com

Information

Grant Agreement N°
225354
Total Cost
€2,942,113
EU Contribution
€2,246,110
Starting Date
01/11/2009
Duration
36 months

Coordinator

PLANUNG TRANSPORT VERKEHR AG
Contact
Dr. Georg Mayer
Planung Transport Verkehr AG
Kriegerstr. 15
D-70191 Stuttgart
Germany
georg.mayer@ptv.de

Dr. Christoph Walther
Planung Transport Verkehr AG
Stumpfstr. 1
D-76131 Karlsruhe
Germany
christoph.walther@ptv.de
www.ptv.de
Website:
www.seron-project.eu

Project objectives

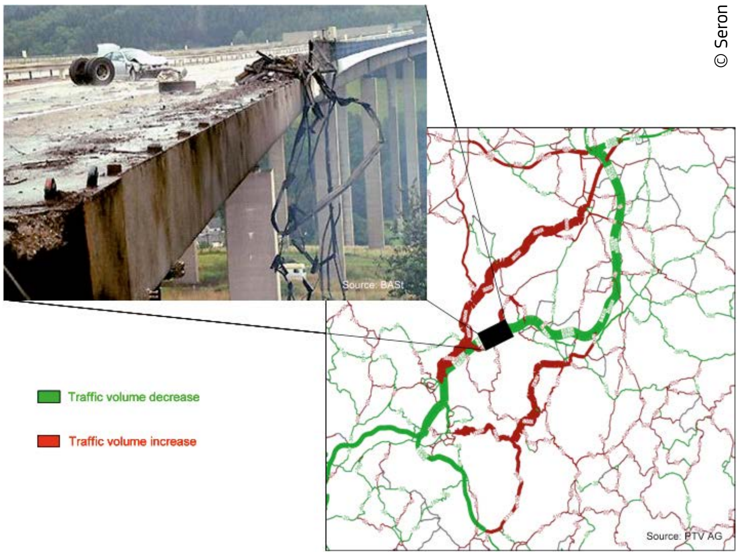
The SeRoN project undertakes a holistic approach at both infrastructure object and road network level. Its main objectives are to investigate the impacts of possible man-made attacks on the transport network, in particular the resulting regional and supra-regional impacts on transport links and their economic impacts. SeRoN focuses on the development and validation of an innovative methodology which is designed to provide a common framework for the analysis of critical road infrastructure objects or road transport networks with regard to their importance within the European transport network and also with regard to possible attacks. This methodology is based on an interdisciplinary interaction of expertise and innovative simulation methods. Furthermore, possible protection measures for critical road transport infrastructures can suitably be chosen and evaluated regarding their impact on security and cost-effectiveness.

Description of the work

First a comprehensive threat analysis for transport infrastructures focusing on man-made attacks is carried out. Then data on relevant infrastructure types and classes of the Trans-European road network is gathered, with so-called "partner regions" being more comprehensively covered. Data provided will be evaluated to identify generic infrastructure types and classes which are critical in terms of vulnerability to man-made attacks, e.g. due to their type of construction, and to classify them based on the risk they are exposed to. The results provide the input data for a knowledge database intended to be a means to manage and maintain categorised critical infrastructures and associated protection measures. Such object information is needed for the calculations at network level analysing the importance of individual infrastructures. Their vulnerability will be determined in probable scenarios, studying the impacts of a failure of critical (parts of) infrastructures and the resulting traffic disturbances using scenario analysis and macroscopic traffic flow models. Network data will include information about location and importance of infrastructures in the road network, traffic loads, etc. Thus critical infrastructures of the road network can be identified and ranked according to priority. The risk assessment includes the impact assessment for the respective infrastructure based on different occurrence scenarios with related event sequences. Vulnerabilities are estimated using the local traffic conditions and simulations, e.g. escape simulations, explosives and smoke propagation simulations. Security improvements will be determined and monetary and economic impacts of different measures examined by means of cost-benefit analyses to identify the most effective security measures. Finally, using a few suitable examples, the new methodology developed will be validated before recommendations for infrastructure owners will be formulated taking into account external expert knowledge gained in workshops.

Expected results

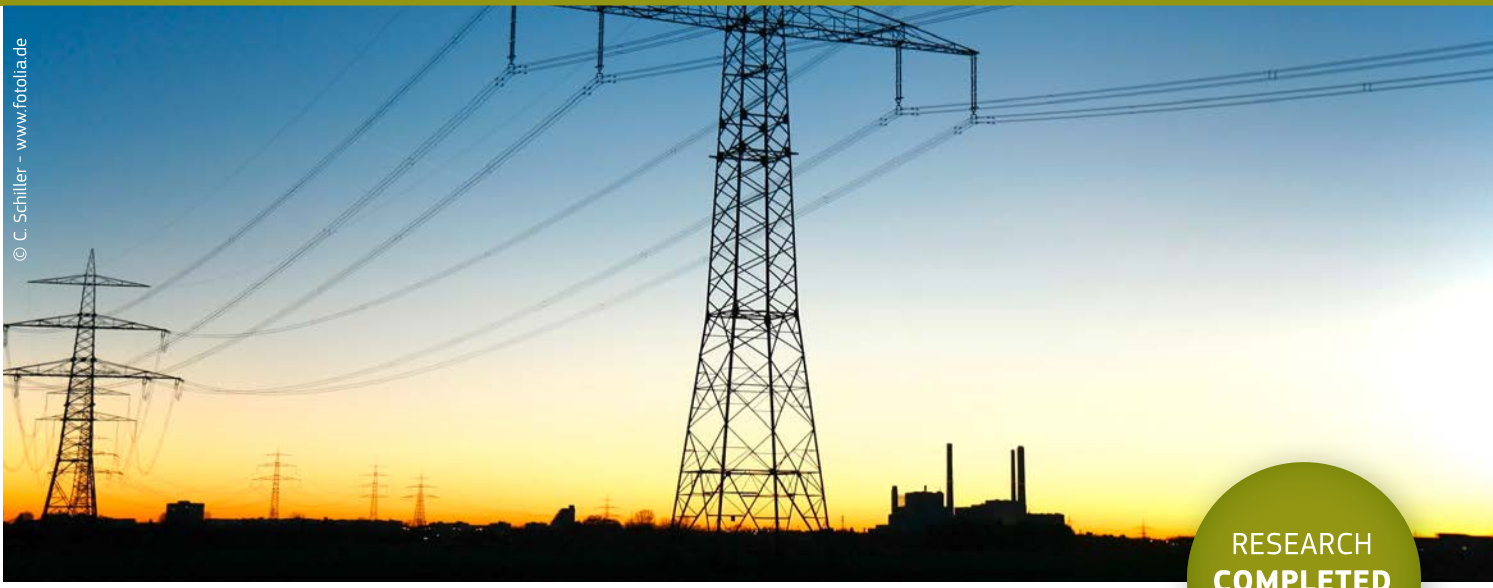
The SeRoN project results include a knowledge database, an innovative methodology and recommendations covering macro-economic, institutional and organisational and technical issues. They will allow infrastructure owners and operators developing strategies to improve the security of transport structures and to select investments in countermeasures and risk mitigation strategies. The developed methodology may be transferred to transport networks used by other traffic modes and to natural disasters.



© Seron

PARTNERS	COUNTRY
Planung Transport Verkehr AG (PTV)	Germany
Bundesanstalt für Straßenwesen (BASt)	Germany
Parsons Brinckerhoff (PB)	United Kingdom
Technische Universität Graz (TU Graz)	Austria
Traficon n.v (TRFI)	Belgium
Ernst Basler und Partner (EBP)	Switzerland
NIRAS Rådgivende Ingeniører og Planlæggere A/S (NIR)	Denmark

SESAME / Securing the European electricity Supply Against Malicious and accidental thrEats



© C. Schiller – www.fotolia.de

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261696
Total Cost
€3,982,815.20
EU Contribution
€2,753,789.80
Starting Date
01/05/2011
End Date
31/08/2014

Coordinator

POLITECNICO DI TORINO
DIPARTIMENTO DI INGEGNERIA ELETTRICA
Corso Duca degli Abruzzi, 24
I-10129, Torino
ITALY
Contact
Prof. Ettore BOMPARD
Tel: +39 011 090 7154
Fax: +39 011 090 7199
E-mail:
ettore.bompard@polito.it

Project objectives

The project targeted two key-issues for the security of the European Electric Power Systems: *the decision making related to the assurance of the security of power systems* as critical infrastructure and the design of a *regulatory framework* that allows for covering the cost of security in a market environment.

The project was developing a Decision Support System for the protection of the European power transmission, distribution and generation system. This Decision Support System can be used to:

» identify the vulnerabilities of the analyzed grid and production plants and detect their origins;

» estimate the damage / impact of real or simulated network failures;

» identify the possible measures for prevention of outages and acceleration of automatic restoration;

» rank these measures according to their effectiveness and their cost-benefit ratios;

» carry out contingency analyses of the transmission and distribution network and the generation facilities.

The project, based on the analysis of the impacts of failures in the supply of energy, was designing a set of regulatory rules, based at the national and coordinated at the European level, aiming at assuring an adequate level of security to the European power grid from an economic point of view.

Description of the work

The first step was to analyse the origin of vulnerabilities and how weaknesses of the power transmission / distribution / generation system can be identified. Therefore, the metrics needed for an exhaustive detection and comprehensive rating of the vulnerabilities are being developed. This project not only considered the physical network, with its control and communication structure, as the potential origin of the vulnerabilities, but also incorporated organisational and educative structures.

The second step was to identify effective measures to specifically address each identified kind of vulnerability and threat. These measures were mainly on a technical level, but also included organisational and educational measures.

The impact of already occurred power interruptions and possible blackout scenarios was then analysed.

The tools developed in the preceding work steps were then integrated into a comprehensive prototype software Decision Support System. In a first step, the tool was assembled and the developed algorithms and metrics implemented. Then, the DSS was tested on two actual power grids of two partner power networks, namely Romania and Austria.

The last work step provided the necessary elements of a comprehensive regulatory policy, which fully incorporated the security of supply.

Results

SESAME developed a decision support system (DSS) for the protection of the European power system and applied it to two regional electricity grids, Austria and Romania. This DSS aimed to:

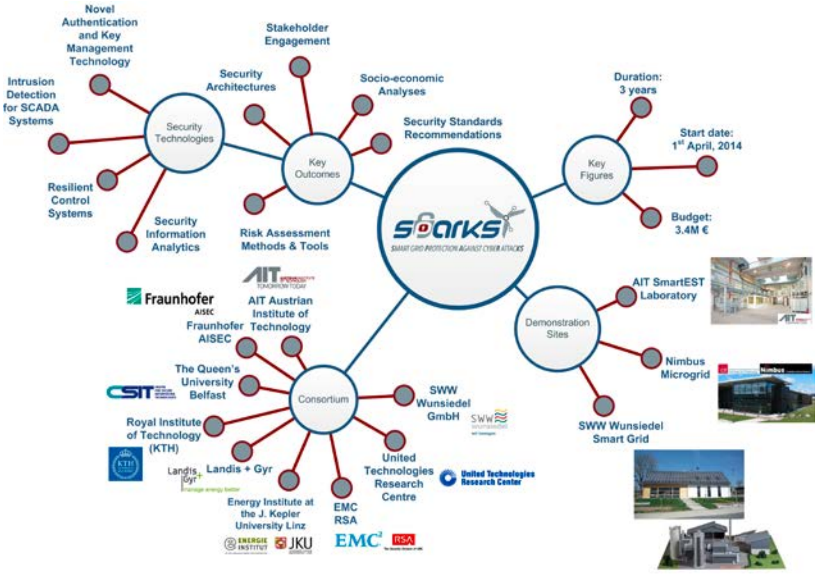
- identify the vulnerabilities and to detect their origins
- estimate the damage/impact of real or simulated network failures
- identify the possible measures for prevention of outages and acceleration of automatic restoration
- rank these measures according to their effectiveness and their cost-benefit ratios
- carry out contingency analyses of the transmission/distribution network and generation facilities

The DSS developed by SESAME can help the main public actors in the power systems – TSOs and Regulators – with their decision making regarding network planning and investment, policies and legislation, and efforts to minimise the impacts (physical, security of supply, and economic) of power outages.

SESAME also developed a best practice and comprehensive regulatory and policy framework for the security of electricity systems. This is structtured around three main dimensions – i.e. economic analysis, technology and innovation policy, and regulatory schemes at both the national and EU level.

PARTNERS	COUNTRY
Politecnico di Torino (PoliTo)	Italy
Energy Institute at the J. Kepler University Linz (EI-JKU)	Austria
Indra Sistemas SA (INDRA)	Spain
Heriot Watt University (HWU)	United Kingdom
e-Control (Ectrl)	Austria
Deloitte (Delo)	Spain
TU Delft (TUD)	The Netherlands
Transelectrica (TrEl)	Romania
Kudos Research (KUDOS)	United Kingdom

SPARKS / Smart Grid Protection Against Cyber Attacks


Novel Authentication and Key Management Technology
Intrusion Detection for SCADA Systems
Security Technologies
Resilient Control Systems
Security Information Analytics
Stakeholder Engagement
Security Architectures
Socio-economic Analyses
Security Standards Recommendations
Key Outcomes
Risk Assessment Methods & Tools
sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS
Duration: 3 years
Start date: 1st April, 2014
Key Figures
Budget: 3.4M €
AIT SmartEST Laboratory
Demonstration Sites
Nimbus Microgrid
SWW Wunsiedel Smart Grid
AIT Austrian Institute of Technology
Fraunhofer AISEC
The Queen's University Belfast
Royal Institute of Technology (KTH)
Landis + Gyr
Energy Institute at the J. Kepler University Linz
EMC RSA
United Technologies Research Centre
SWW Wunsiedel GmbH
Consortium

Grant Agreement N°
608224
Total Cost
€4,913,955.40
EU Contribution
€3,429,551.00
Starting Date
01/04/2014
Duration
36 months

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)
SAFETY &
SECURITY DEPARTEMENT
DONAU-CITY-STRASSE 1
1220 VIENNA, AUSTRIA
Contact
Dr Paul Smith
Tel: +43 664 88390031
Fax: +43 50550 2813
E-mail: paul.smith@ait.ac.at
Website:
https://project-sparks.eu

Project objectives

The aim of the SPARKS project is to promote awareness of existing and emerging smart grid cyber-security risks to stakeholders, including energy network operators, industry and policy makers. It will develop procedural and technical countermeasures, and provide cost assessments of key smart grid security technologies that are developed in the project. The project will also investigate privacy issues related to smart grid development.

Description of the work

The project will investigate risk assessment methods that are tailored to the smart grid. Tools will be developed to support these methods, including a novel cyber-attack simulation environment that can be used to measure the impact of an attack. Moreover, SPARKS will make recommendations about security architectures and standards for smart grids.

A number of key security technologies and measures will be developed via a set of mini-projects:

» cyber-attack resilient control systems,

» real-time network monitoring of SCADA-based control systems,

» novel hardware security technologies for smart metering applications, and

» security analytics techniques for smart grid.

Business cases for these technologies will be developed to support the case for their deployment. Additionally, the societal acceptance of smart grid security technologies will be investigated, along with the legal directives and regulatory requirements.

The research outcomes of the project will be demonstrated in a number of testbed and real-world deployment facilities. There will be a series of workshops across the project's lifetime to engage with stakeholders.

Expected results

The main impact of the SPARKS project is ensuring the security and resilience of future smart grid infrastructures.

SPARKS will deliver important new knowledge about vulnerabilities, attack vectors, security risks, legislation, and consequential costs to business and society.

To maximise our impact, SPARKS has identified a number of technology development areas that offer significant advances in the state of the art. With experienced technology experts working in the domains of SCADA intrusion detection, new methods for smart meter authentication, security information analytics and resilient power control systems, SPARKS will deliver impact right across the smart grid spectrum.

PARTNERS	COUNTRY
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung e.V (Fraunhofer AISEC)	Germany
Queen’s University Belfast (QUB)	United Kingdom
Energieinstitut an der Johannes Kepler Universität Linz (EI)	Austria
EMC Information Systems International Ltd (EMC)	Ireland
Kungliga Tekniska Hoegskolan (KTH)	Sweden
Landis + Gyr AG (L+G)	Switzerland
United Technologies Research Centre Ireland, Limited (UTRC)	Ireland
SWW Wunsiedel GmbH (SWW)	Germany

STAR-TRANS / Strategic risk assessment and contingency planning in interconnected transport networks

© Jean-Paul Bounine - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225594
Total Cost
€3,296,369.71
EU Contribution
€2,105,588.94
Starting Date
01/11/2009
End Date
30/04/2012

Coordinator

INTRASOFT INTERNATIONAL S.A.
RUE NICOLAS BOVÉ
1253 LUXEMBOURG
LUXEMBOURG
Contact
Dr. Antonios Ramfos
E-mail: antonis.ramfos@intrasoft-intl.com
Website:
www.startrans-project.eu

Project objectives

The fundamental assumption within STAR-TRANS is that transportation assets, such as airplanes and tunnels, are an integral part of larger systems. Taken together, individual transportation networks form a "network of networks". This provides a basis for an integrated EU-wide approach to risk management in transportation networks that would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States.

STAR-TRANS' contribution to the risk assessment process in transportation networks is the recognition of the importance that the impact of a risk incident might have on the assets of the whole 'network of networks'.

The project outcome will offer important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences, (cost, timing, resources, etc.) of proposed actions.

A specialised software system will be developed that will support the end users' and network operators' needs.

The objectives of the STAR-TRANS project are:

To produce a security risk assessment framework for European interconnected and interdependent transportation networks and to evaluate the proposed risk assessment framework in two cities.

Description of the work

The aim of the proposed transportation security risk assessment framework is to formalise the linkage between risk incidents, transportation network assets and dependency types between assets in order to assess the impact of an incident on the affected interconnected and interdependent networks at the 'network of networks' level. In particular, STAR-TRANS intends to:

» formalise the impact assessment process at the 'network of networks' level;

» develop ICT tools that support the formalised impact assessment process; and

» trial & evaluate the developed impact assessment process and tools.

STAR-TRANS' comprehensive risk assessment approach targets the security operation of the European transport networks. STAR-TRANS will be guided by a holistic risk assessment methodology for critical infrastructure for the analysis and assessment of common issues for risks, threats and vulnerabilities.

Within the STAR-TRANS framework, security risk in the integrated transportation networks will be defined as the combination of:

» *Vulnerability*, reflecting the possibility of a risk incident, e.g. terrorist attack, for the interdependent and interconnected European transport networks, compared to the possibility of protecting them through inherent or managed safeguards;

» *Consequences* of a successful attack, which is defined using (i) the possible number of casualties / fatalities, (ii) disruption and recovery time and (iii) the economic impact.

The combined approach of various transport networks in one risk assessment tool will allow for easy information exchange between different networks and infrastructure elements / facilities.

Results

STAR-TRANS created models that can represent possible risk incidents, the structure and assets of Europe's heterogeneous transport systems, and the relationship between the different assets in the networks. In this regard, the project developed a STAR-TRANS modelling language and an impact-assessment modelling language.

PARTNERS	COUNTRY
INTRASOFT International SA	Luxembourg
National Centre for Scientific Research Demokritos - Environmental Research Laboratory	Greece
Center for Security Studies	Greece
Confederation of Organisations in Road Transport Enforcement	Belgium
QinetiQ SA	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)	Germany
Centre for Research and Technology Hellas - Informatics & Telematics Institute	Greece
Metropolitan Police Service	United Kingdom
CTL Cyprus Transport Logistics Ltd	Cyprus
SQUARIS Ltd	Belgium
SOCIETA RETI E MOBILITA SPA (SRM)	Italy

STRUCTURES / Strategies for the Improvement of Critical Infrastructure Resilience to Electromagnetic Attacks

© Thinkstock

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285257
Total Cost
€4,797,731.63
EU Contribution
€3,497,673.54
Starting Date
01/07/2013
End Date
31/10/2015

Coordinator

INGEGNERIA DEI SISTEMI S.P.A. (IDS)
Business Development
VIA FLAMINIA, 1068
00189 ROME,
ITALY
Contact
Aldo Bonsignore
Tel: +39 0633217414
Mobile: +39 3357458088
Fax: +39 0633217402
E-mail: a.bonsignore@idscorporation.com
Website:
http://www.idscorporation.com

Project objectives

The project aimed to understand the level of risk produced by intentional electro-magnetic interference to critical infrastructures and to provide guidelines for their protection. It is focused on the following functions:

- Risk assessment, modelling and impact reduction
- Situation awareness and assessment
- Within the framework of "Risk assessment, modelling and impact reduction", the research focuses on the following main capabilities and technologies:

a. Capabilities

- Classification of intentional electromagnetic environments (radiated and conducted);
- • Classification of critical infrastructures with respect to by intentional electro-magnetic interference threats;
- Risk assessment of the occurrence of threat events and their most likely modalities;
- Classification of e.m. susceptibility levels of equipment, systems and infrastructures;
- Validated electromagnetic modelling tools for risk assessment and design;
- Dedicated measurements (mainly to estimate IEMI susceptibility levels and to validate modelling algorithms);
- Investigation of current protection effectiveness;
- Optimal design criteria to make infrastructures more robust against interference threats, including shielding for structures, systems, sub-systems etc.
- Design of components and strategies for protection (with preference given at first to low cost solutions);
- Pre-regulatory and organisational material to support parties affected by by intentional electro-magnetic interference and for policy makers re: recommendations, guidelines, methodologies, and procedures (e.g. regarding shell materials and redundancy architectures).

b. Technologies

- EMC evaluation and hardening;
- intentional electro-magnetic interference measurements;
- Simulation tools for analysis (risk assessment) and design (protection improvement);
- Structural and smart materials able to improve protection against intentional interference

Description of the work

STRUCTURES was based on 11 work packages (WPs).

Scenario assessment was done by WP2 and WP3, while WP4 and WP5 assessed analytical/modelling and experimental methodologies and their preparation for the next phase of "risk investigation and protection measures assessment".

WP6 performed experimental activities to characterise susceptibility thresholds to intentional electro-magnetic interference and to provide test cases for the modelling procedures. Other packages investigated protection technologies and strategies, and electro-magnetic interference sensors and sensor networks suitable for night and day and all-weather monitoring of the infrastructure environment.

WP10 developed guidelines and recommendations for policy makers, standard bodies and critical infrastructures. A "safety risk assessment" approach was applied, based on:

- Identification of the likelihood and severity of adverse consequences resulting from an electro-magnetic interference hazard;

- Application of a suitably calibrated safety risk assessment matrix and severity scale;
- Assessment of risk tolerability;
- Assessment of accessibility and other factors which may affect the vulnerability of infrastructure.
- Identification of possible mitigating actions;
- Updating of the risk assessment matrix.
- Also the companion disciplines and standards for Critical Infrastructure's protection such as the "Business Continuity Management" approach and the ICT standards for Security Techniques were considered to situate the guidelines in a larger existing frame regarding critical infrastructures.

Results

The project attained better comprehension of the problems and risks related to intentional electro-magnetic interference attacks to critical infrastructures

Guidelines and recommendations for policy makers, standard bodies and critical infrastructures operators were also defined.

Viable solutions to estimate and reduce risk will be made available to policy makers and critical infrastructure managers.

PARTNERS	COUNTRY
Ingegneria Dei Sistemi S.p.A (IDS)	Italy
Ecole Polytechnique Fédérale de Lausanne (EPFL)	Switzerland
Haute Ecole Spécialisée de Suisse Occidentale (HES-SO)	Switzerland
The University of York (UoY)	United Kingdom
MONTENA technology sa (Montena)	Switzerland
Helmut-Schmidt- Universität (HSU)	Germany
Leibniz Universität Hannover (LUH)	Germany
Bergische Universität Wuppertal (BUW)	Germany
Bergische Universität Wuppertal (RWM)	Germany
University of Twente (UT)	The Netherlands
Istituto Superiore Mario Boella (ISMB)	Italy
Navigate Consortium (NAVI)	Italy

TASS / Total airport security system

© josh webb - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241905
Total Cost
€14,966,370.60
EU Contribution
€8,986,696.15
Starting Date
01/04/2010
End Date
31/03/2014

Coordinator

VERINT SYSTEMS LTD
Business Development
33 Maskit st
46733 Herzlia, Israel
Contact
Hazzani Gideon
Tel.: +972 9 9622596
Mobile:+972 54 778 2596
E-mail:
Gideon.hazzani@verint.com
Website: www.tass-project.eu

Project objectives

Airports, airplanes and air travellers are often the targets of terrorists, a reality that poses many security challenges and requires a variety of security systems. The EU-funded project TASS – "Total airport security system" – was addressing these threats through the development of a sophisticated surveillance system that represents a security monitoring solution for an entire airport. The system was being designed to enhance the efficiency and reliability of security screening while protecting the privacy and rights of airport passengers.

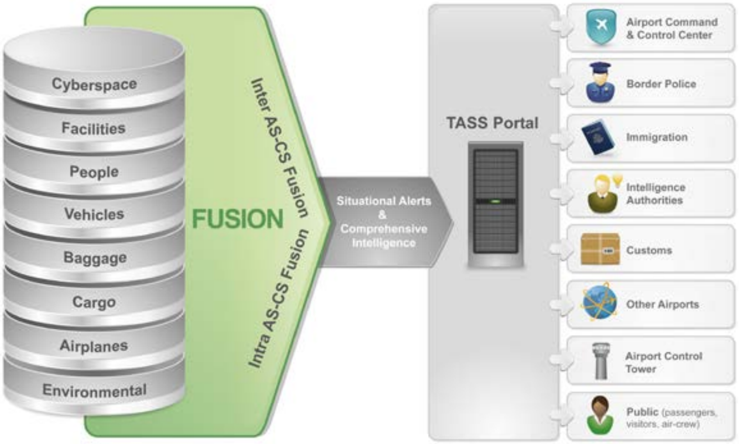
Description of the work

Offering real-time situational awareness of all airport facilities and surroundings – including people, vehicles, cargo and airplanes – the system ccollected and analysed data from different sources and technologies. It featured three main components: the front end, the data fusion and mediation system, and portal/back-end applications. The portal displayed all security and transport information, and notified authorities to execute decisions rapidly. It also minimised errors and false alarms.

So far, the project team has progressed well towards developing the system. After having mapped and classified potential threats to airports, it outlined the required technologies, designed the system's architecture and adapted its front-end systems to airport environments. This has yielded a full ready-to-use TASS prototype. Testing took place at Heathrow International Airport in the United Kingdom in a complex system that combined many different components and systems. These ranged from various kinds of sensors and global position system tracking technologies to radio-frequency identification systems and an unmanned ground vehicle.

Results

With its integrated approach to airport security, TASS has effectivly created a comprehensive airport security intelligence solution that offers accurate real-time situational awareness to airport authorities. Once finalised and commercialised, the solution promises to become an important alternative to current airport security systems. It will help thwart terrorist attacks, minimise injuries and save lives wherever it is implemented, making the world's airports safer than ever.



© Tass

PARTNERS	COUNTRY
Verint Systems Ltd (VRNT)	Israel
BAA Limited (BAA)	United Kingdom
Grupo Mecanica del Vuelo Sistemas S.A. (GMV)	Spain
Rapiscan Systems Limited (RSL)	United Kingdom
Consorzio per la Ricera Nell' Automatica e Nelle Telecomunicazioni C.R.A.T (CRAT)	Italy
National Center for Scientific Research "Demokritos" (NCSR "D")	Greece
GMVIS Skysoft SA (SKY)	Portugal
Mentum SA (MTM)	France
Vitrociset Spa (VITRO)	Italy
Alcatel-Lucent Italia S.P.A (ALI)	Italy
The Provost Fellows & Scholars of the College of the Holy and Undivided Trinity of Queen Elizabeth near Dublin (TCD)	Ireland
IMEGO AB (IMEGO)	Sweden
Elbit Security Systems ltd (ELSEC)	Israel
Athens International Airport SA (AIA)	Greece
Real Fusio France (RF)	France
Immersion SAS (IMM)	France
Red-M Wireless Ltd. (RED-M)	United Kingdom
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Ernst & Young (Israel) Ltd (EY)	Israel
ANA - Aeroportos De Portugal, SA (ANA)	Portugal
INOV, Inesc Inovacao, Instituto De Novas Tecnologias (INOV)	Portugal

XP-DITE / Accelerated Checkpoint Design Integration Test and Evaluation

© Thinkstock

Information

Grant Agreement N°
285311
Total Cost
€14,613,264.82
EU Contribution
€9,992,634.87
Starting Date
01/09/2012
Duration
55 months

Coordinator

NETHERLANDS ORGANISATION FOR APPLIED SCIENTIFIC RESEARCH (TNO)
Safety and Security Research
LANGE KLEIWEG 137
PO BOX 45
2280 AA RIJSWIJK,
THE NETHERLANDS
Contact
Mark van den Brink
Tel: +31 8886 63898
Mobile: +31 6 3015 8707
Fax: +31 8886 66938
E-mail:
mark.vandenbrink@tno.nl

Project objectives

The aim of the XP-DITE project is to develop, demonstrate and validate a comprehensive, passenger-centred approach to the design and evaluation of integrated security checkpoints at airports.

A key element of the project is the development of a design tool that allows the design of innovative new checkpoints and modification of existing checkpoints to meet combinations of overall system level requirements. Another major deliverable comprises a validated set of protocols and tools for evaluating the performance of the checkpoint, again at the system level.

Description of the work

Airport Checkpoint (ACP) requirements at overall checkpoint system-level are determined for security, operational, passenger perception and ethical aspects. A conceptual model is developed to enable development of the design process and evaluation platform. All requirements are assessed by the XP-DITE advisory board, expert groups and ethical advisory group.

A design process and supporting software (Design Tool) based on the conceptual model and overall system requirements will be developed. The design process is foreseen to be used for the creation or adaptation of an airport checkpoint and for the assessment of new technologies.

Computational evaluation methods at system or checkpoint level will build on the conceptual model. The aim is to quantify the overall performance from the properties of all the components involved. An experimental evaluation method for checkpoints will be developed with the aim of proposing a standard on-site test prescription for checkpoints applicable to any EU airport. Both computational and experimental methods will be combined into a single interface, the Shared Evaluation Platform (SEP), allowing for easy facilitation and evaluation of checkpoints at system level.

Proofs-of-concept airport checkpoint will be integrated and installed at Schiphol Airport and Manchester Airport. To fully demonstrate and exploit the capabilities of the XP-DITE results, not only commercial off-the-shelf components but also mature, close-to-market-introduction technologies will be developed. The results of the tests at airport and laboratory scale are given as feedback to the Design Tool and the SEP.

The results of the project will be disseminated widely and actively into the European security community by different means, such as websites, brochures, publications, conferences and workshops.

Expected results

The XP-DITE approach will allow airports, checkpoint designers and regulators to incorporate a wide range of requirements and to evaluate checkpoint performance against security performance, cost, throughput, passenger satisfaction and ethical factors. This will help ensure robust and controllable aviation checkpoint security performance, whilst providing freedom for airport operators to design checkpoints with innovative technologies and procedures.

All extra time spent at the airport has a cost. It means less time to spend at work, with children and for leisure. There are also secondary effects from the delays that create new costs. For example, longer delays at the airport encourage passengers to seek new modes of transportation for their trips, such as driving, that are less safe.

XP-DITE will have a positive impact in this respect by showing the way and handing the tools to reduce airport checkpoint delays, even with improved security.

Now security operations at European airports account for about 35 per cent of operating costs. These costs are either born by the passenger or else by the taxpayer. In many Member States, airports pay for their own security measures; in others the government picks up the tab. The total societal costs of security measures are even higher when factors such as delays, time needed to screen passengers at airports, and non-monetary costs such as privacy concerns or ethics balancing are considered.

XP-DITE will show that advanced, customer friendly and cost-effective security checkpoints can be achieved by adopting a unified approach on design and evaluation of airport checkpoints, introducing new system-level performance requirements.

PARTNERS	**COUNTRY**
Netherlands Organisation for Applied Scientific Research (TNO)	The Netherlands
Fraunhofer-gesellschaft zur Foerderung der angewandten Forschung (Fraunhofer)	Germany
Swedish Defence Research Agency (FOI)	Sweden
Ingeniera de Sistemas para la Defensa de Espana (ISD)	Spain
Schiphol Nederland (AAS)	The Netherlands
Morpho (MPH)	France
Smiths Heimann (SMI)	Germany
Eurofast SARL (IDP)	France
Iconal Technology (ICO)	United Kingdom
Cascade Technologies (CAS)	United Kingdom
Alfa Imaging (ALF)	Spain
Albert-Ludwigs-Universitaet Freiburg (UNF)	Germany
The Manchester Airport Group (MAN)	United Kingdom

CORE / Consistently Optimised Resilient Secure Global Supply-Chains

Information

Grant Agreement N°
603993
Total Cost
€48,831,356
EU Contribution
€29,254,829
Starting Date
01/05/2014
Duration
48 months

Coordinator

EUROPEAN SHIPPERS' COUNCIL (ESC)
Rond Point Schuman, 6
1000 Brussels BELGIUM
Contact
Nik DELMEIRE
Tel: +32 494 56 07 07
Mobile: +32 494 560707
E-mail: n.delmeire@europeanshippers.eu
Website: www.coreproject.eu

Project objectives

CORE will demonstrate how a powerful and innovative Consistently Optimised REsilient ecosystem's implementation, integrating interoperability, security, resilience and real-time optimisation can produce cost effective, fast and robust solutions for efficient and secure transit of goods through the global supply chain.

It will show how the supply chain's protection and a reduction of its vulnerability to disruption (by natural disasters, terrorism, theft, etc.), can be done while guaranteeing a timely, efficient flow of commerce across EU and other regions of the world – while bearing in mind the benefits for stakeholders (transaction, transport, regulatory and financial operators).

Using CORE's real-time optimisation tools, security and tracking data will be integrated into supply chain operations with a view to efficiency and environmental impact. CORE will offer solutions that cover all levels of time granularity, ranging from strategic models to dynamic daily plans and real-time scheduling and optimisation. These will help operators create resilient contingency plans and to react to unexpected events to avoid serious economic collapse.

CORE will address:

1. End-to-end supply chain security based on standardization, harmonization and mutual recognition;

2. Controlled global visibility of security risks and other supply chain threats and their impact on supply chain flows around the world;

3. Real-time "Lean Agile Resilient Green Optimised" supply chain solutions for supply chain resilience against high-impact events

The results of CORE will help the EU introduce changes to Customs policy to achieve a balance between public and business interests, within reasonable regulatory constraints. The idea of changing Customs reporting procedures "from push to pull" using secure data pipelines for the whole value-and-transport chain has already begun in a number of previous EU-funded projects. CORE will more broadly demonstrate this approach by addressing security and supply chain optimisation. It will generate a security and supply chain resilience ecosystem to operate in an international context that supports implementation of EU security and information management policies.

CORE's "Supply Chain Security Reference Model" (SCSRF) will establish the basis for standardisation of secure transport & logistics as part of an integrated framework of trusted worldwide networks. Its Ecosystem will offer a distributed socio-technical system based on self-organisation, scalability and sustainability. It will include data, knowledge, best practices and services that can easily be plugged into existing IT systems to yield enhanced security, resilience and efficiency.

Description of the work

1. Requirements analysis and impact assessment.

2. SCS Controls and Integration Services

3. Create end-to-end supply chain security via a multi-method threat and vulnerability analysis capability.

4. Provide supply chain situational awareness tools & maps that build on data and results from reference projects to satisfy Customs and business requirements for reliable, accurate, complete data

5. Provide real-time "Lean Agile Resilient Green Optimised" (LARG+O) supply chain planning

6. Provide a supply chain security reference framework harmonised with the common framework produced in the e-Freight and other reference projects

7. Provide a CORE connectivity infrastructure and solutions development environment

8. Provide an supply chain security (SCS) ecosystem dedicated to the needs of SCS communities based on infrastructure services that amplify the capabilities of CORE components.

9. Demonstrators. CORE demonstrators will validate the applicability and benefits of the project's approach via scenarios characteristic of the global supply chain

10. Stakeholder engagement, knowledge diffusion and sustainable development

Expected results

End-to-end supply chain security facilitating standardization, harmonization and mutual recognition

Security Situational Awareness Maps to enhance the visibility of threats and exposure of flows

Real-time Lean Agile Resilient Green Optimised (LARG+O) supply chains

PARTNERS	COUNTRY
European Council Of Transport Users (ESC), Customs Co-Operation Council (WCO), Clecat - European Association for Forwarding, Transport, Logistics and Customs Service (CLE), IRU Projects ASBL (IRU), European Intermodal Association (EIA), Service Public Federal Finances (BC), Descartes Systems (BELGIUM) (DESC), JRC -Joint Research Centre- European Commission (JRC), VLTN GCV (VLTN), Logit Systems BVBA (LOGIT), Seabridge NV (SB), Procter & Gamble Services Company Nv (P&G), European Organisation For SecuritySCRL (EOS)	Belgium
The International Criminal Police Organization (IPOL), Ministere De L'ecologie, du Developpement Durable et de L'energie (MEDDE), Smiths Heimann SAS (SMH), Advanced Track And Trace SA (ATT), CONEX SA (CX)	France
Cooperatieve Bloemenveiling Floraholland U.A. (FH), Ministerie Van Financien Directoraat Generaal Belastingdienst (DCA), Ministerie Van Binnenlandse Zaken En Koninkrijksrelaties (KLPD), Nederlandse Voedsel En Warenautoriteit (NVWA), Seacon Venlo Expeditie B.V. (SEA), Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO), Technische Universiteit Delft (TUD), Logistiek Zonder Papier BV (LZP), Technische Universiteit Eindhoven (TUE)	The Netherlands
Dhl Exel Supply Chain Spain SL (DHL), Terminal Maritima De Zaragoza SL (TmZ), Portic Barcelona S.A (POR), Fundacion Zaragoza Logistics Center (ZLC), Enide Solutions .S.L (NIDE), ATOS Spain SA (ATOS), Trans SESE Sociedad Limitada (SESE), Bsh Electrodomesticos Espana SA (BSH)	Spain
HM Revenue And Customs (HMRC), METRO SHIPPING LIMITED (MET), BAP Logistics Ltd (BAP), Maritime Cargo Processing PLC (MCP), BMT Group Limited (BMT), INLECOM Systems Ltd (ILS), MJC2 Limited (MJC2), CLMS (UK) LIMITED (CLMS), Security Projects Uk Limited (SEP), Uniserve (Holdings) Limited (Uni),	United Kingdom
Italian Ministry of Infrastructure and Transports (MIT), Consorzio Ib Innovation (IBI), La Spezia Container Terminal SPA (LAS), Telespazio SPA (TPZ), So.Ge.Mar. Societa Generale Magazzini Raccordati Interporto SPA (SOG), TTS Italia (TTS), Majorca SPA (MAJ), Click & Find S.R.L (C&F), Ceramiche Caesar SPA (CC)	Italy
dbh Logistics IT AG (dbh), Senator fuer Wirtschaft und Haefen Bremen (SEPL), Institut Fuer Seeverkehrswirtschaft Und Logistik (ISL)	Germany
Intrasoft International SA (INT)	Luxembourg
A.P. Moller - Mærsk A/S (MAER), Copenhagen Business School (CBS)	Denmark
Instytut Logistyki i Magazynowania (ILiM)	Poland
Conceptivity SARL (CPT), Cross-border Research Association (CBRA), Hoyer (Svizzera) SA (Hoyer)	Switzerland
Totalforsvarets Forskningsinstitut (FOI)	Sweden
eBOS Technologies Ltd (eBOS)	Cyprus
Center For Security Studies (KEMEA)	Greece
Georgia Tech Research Corporation (GT), iControl Incorporated (iCON)	The United States
Brimatech Services GMBH (BRI)	Austria
Sunwell Technologies INC (SUN)	Canada

IMCOSEC / IMprove the supply chain for COntainer transport and integrated SECurity simultaneously

© Netfalls - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242295
Total Cost
€1,142,591
EU Contribution
€930,718
Starting Date
01/04/2010
End Date
31/03/2011

Coordinator

TSB INNOVATIONSAGENTUR BERLIN GMBH / BEREICH FAV
Fasanenstr. 85, 10623
Berlin
Germany
Contact
Markus Podbregar
Tel: +30 46302 579
Office: +30 46302 563
Fax: +30 46302 588
E-mail: mpodbregar@fav.de
Website: www.imcosec.eu

Project objectives

This project's main aim was to define a basic concept and strategic roadmap for a large scale Demonstration project for security of supply chains to reconcile the global transportation sector's two conflicting trends: free trade vs transport security.

IMCOSEC opted for an approach that minimises the impact of cost and time, thus making it practicable for commercial operators and enterprises, while creating a "win-win" solution between industry and regulatory authorities. Its concept reached for security that balances effectiveness with practicality within a regulatory framework.

The project analysed security regulations, standards and trends, identified security gaps via a generic model of supply chains based on resilience and threat "trees" or charts, referenced security projects, technologies and industry needs and, finally, defined a roadmap for demonstration activities.

Results

The results of IMCOSEC's six work packages can be summarised as the following:

» A generic transport model was created to represent the essential processes and activities of inter-modal transport chains;

» The security aspects of 42 national and international security programmes were compared to determine what new procedures, if any, were needed for the future Demonstration project. IMCOSEC's researchers concluded that no new regulations are needed, but mutual recognition and standardization among national governments should be the goal;

» Security threats along supply chains were identified and folded into a matrix tool that reflects inter-dependencies and interactions between different supply chain arrangements and each kind of threat. The matrix enables threats to be weighted in importance;

» The project's gap analysis to identify the weakest points of the supply chain concludes there are very few single measures that can improve security and efficiency at the same time. However, it argues that a combination of measures could improve both, thus increasing the competitiveness of both industry and the supply chain;

» IMCOSEC's analysis of security projects, technologies and industry needs revealed that many projects focus on either security or efficiency, but not on security and efficiency at the same time. As for technology, it concludes that the most cost-effective and logical combination of technologies to track cargo shipping would be mobile phone-based ones for the identification, positioning and communications;

» Finally, the project's road-map rests on two broad conclusions. First, it insists that human factors (e.g. employee selection, recruitment and training criteria, responsibility for identification and control processes, etc.) are the biggest issues for supply chain security. "This is of primary importance to successfully reduce the other gaps," says IMCOSEC.

Second, it says security-efficiency measures should take into account the views of all supply chain stakeholders, including shipping consignors and consignees, while promoting technologies that use international standards.

PARTNERS	**COUNTRY**
TSB Innovationsagentur Berlin GmbH (FAV)	Germany
International Container Security Organisation (ICSO)	Belgium
Union Internationale des sociétés de transport combiné Rail Route (UIRR)	Belgium
Bureau International des Containers et du transport intermodal (BIC)	France
CBRNE Ltd (CBRNE)	United Kingdom
Studiengesellschaft für den kombinierten Verkehr e.V. (SGKV)	Germany
Politecnico di Milano (POLIMI)	Italy
Technischen Universität Hamburg-Harburg (TUHH)	Germany
Institut für Seeverkehrswirtschaft und Logistik (ISL)	Germany

IPATCH / Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics

Information

Grant Agreement N°
607567
Total Cost
€4,181,126
EU Contribution
€2,976,845
Starting Date
01/04/2014
Duration
36 months

Coordinator

BMT GROUP LTD (BMT)
Research Directorate
Goodrich House
1 Waldegrave Road
Teddington
TW11 8LZ
United Kingdom
Contact
Tom Cane
Tel: +44 (0) 20 8943 5544
Mobile:
+44 (0) 7500 871 748
E-mail:
tcane@bmtmail.com
Website: www.bmt.org

Project objectives

IPATCH addresses the issue of modern piracy and the challenges faced by merchant shipping in keeping crews safe whilst minimising costs. IPATCH will provide ships with new technology for enhanced early detection of piracy threats and real-time decision support for utilising countermeasures appropriately, effectively and safely if they come under attack.

The end of the 20th century has seen an unprecedented resurgence in piracy. In particular, the breakdown of governments and the ensuing lack of "law and order" in African nations have transformed the Gulf of Aden and, more recently, the Gulf of Guinea into some of the world's most dangerous places for commercial and private vessels. Piracy is also on the rise in other regions of the world, including South East Asia and South America. The international community has reacted to these threats with an increased military presence, but the immense costs of these operations demand that further non-military options need to be explored.

Recent years have seen an increase in the use of private maritime security companies on board ships. Whilst effective, these companies often act in a legal "grey area", and the high cost and risk of escalation of violence means they are not a viable solution for all shipping companies. More generally, a comprehensive analysis of available countermeasures is lacking, and inappropriate use can result in unnecessary extra cost for shipping companies and can actually place the ship and its crew at further risk.

Description of the work

IPATCH seeks to address these challenges by first performing an in-depth analysis of the effectiveness and costs – including the legal, ethical and societal implications – of piracy countermeasures. This analysis will be based on historical data, expert knowledge and consultation with shipping companies and other stakeholders.

The results from this analysis will be compiled in a manual to provide well-founded and quantified recommendations to the industry, extending and complementing the IMO's Best Management Practices.

Finally, IPATCH will develop an onboard system for the early detection and classification of piracy threats with a decision support tool to assist the crew in making critical decisions on what actions to take for a given scenario. The IPATCH onboard system will consist of three elements:

» A sensor suite, incorporating existing surveillance capabilities of the vessel (e.g. radar, AIS), and extending and complementing them with the use of advanced visual, thermal and infrared cameras.

» A threat recognition system which fuses data from various sensors and employs new detection, tracking and situational awareness algorithms to give early warning of piracy threats to the captain and crew.

» A decision support tool, which provides real-time situation information to the captain and crew and helps them select the most appropriate countermeasures and best course of action to take to protect the ship and crew from piracy threats as they develop, based on the knowledge captured at the beginning of the project.

The development of the system will take as its starting point the architecture developed in the FP7 project ARENA, which focused on the detection and classification of threats to mobile assets, specifically land-based trucks. In IPATCH, the ARENA platform will be refined and adapted for specific use in the maritime domain.

Towards the end of the project, a demonstration of automated detection and decision support for piracy threats will be carried out on board a real vessel and threat scenarios will be simulated in order to evaluate the performance of different aspects of the system.

Expected results

IPATCH will provide:

- A knowledge base that consolidates historical data on piracy incidents from heterogeneous sources, covering details on the attack, the defensive actions of the vessel, and the ensuing costs and impacts. The information will be augmented with evaluations of the legal, ethical, societal and economic implications of different countermeasures.
- A manual on the use and implementation of countermeasures against piracy based on results from the historical analysis and stakeholder consultations.
- An onboard system for the early detection and classification of piracy threats, building on the architecture from the ARENA project.
- A maritime data set, comprising a collection of fully annotated and documented sensor data from realistic simulated piracy environments, to enable the development and performance evaluation of maritime threat detection algorithms. The dataset will be published for the benefit of both the maritime and research communities.

PARTNERS	COUNTRY
BMT Group Ltd (BMT)	United Kingdom
Totalforsvarets Forskningsinstitut (FOI)	Sweden
University of Reading (UoR)	United Kingdom
ITTI Sp. z o.o. (ITTI)	Poland
Università Cattolica del Sacro Cuore (UCSC)	Italy
Sagem Défense Sécurité (SAG)	France
Termisk Systemteknik i Sverige AB (TST)	Sweden
Université de Namur ASBL (UoN)	Belgium
Foinikas Shipping Company NE (FNK)	Greece

LOGSEC / Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security

© Kaarsten - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241676
Total Cost
€800,047
EU Contribution
€753,372
Starting Date
01/04/2010
End Date
31/03/2011

Coordinator

EFP CONSULTING (UK) LTD.
MOTHERWELL
BRANDON STREET -
OAKFIELD HOUSE
ML1 1XA
UK
Contact
Dana Remes
Phone: +44 141 649 3244
E-mail:
dana@efpconsulting.com
Website: www.logsec.org

Project objectives

The LOGSEC project had the following three main objectives:

- To deliver a strategic roadmap for supply chain security in Europe; roadmap depicting possible security gaps and responsibility backlogs between different operators, both business and governmental.
- To address relevant political, policy, regulatory, technology and service aspects, together with their combinations and to define the ones most critical in security research.
- To combine global supply chain management expertise and technological expertise with crime prevention expertise to improve real security in end-to-end supply chains, in a cost-efficient manner.

Description of the work

The LOGSEC project team consisted of organisations with in-depth experience in European and global supply chain security research and technology analysis and partners representing a broad set of European shippers and logistics operators and customs administrations. Key technologies and procedural aspects covered by the project include: container and goods/inventory, authentication, traceability, inspection and monitoring technologies; risk assessment systems and models; Information transfer systems; Intermodal transport security; modernisation of customs procedures; protection of supply chain infrastructure. User requirements and data collection steps included:

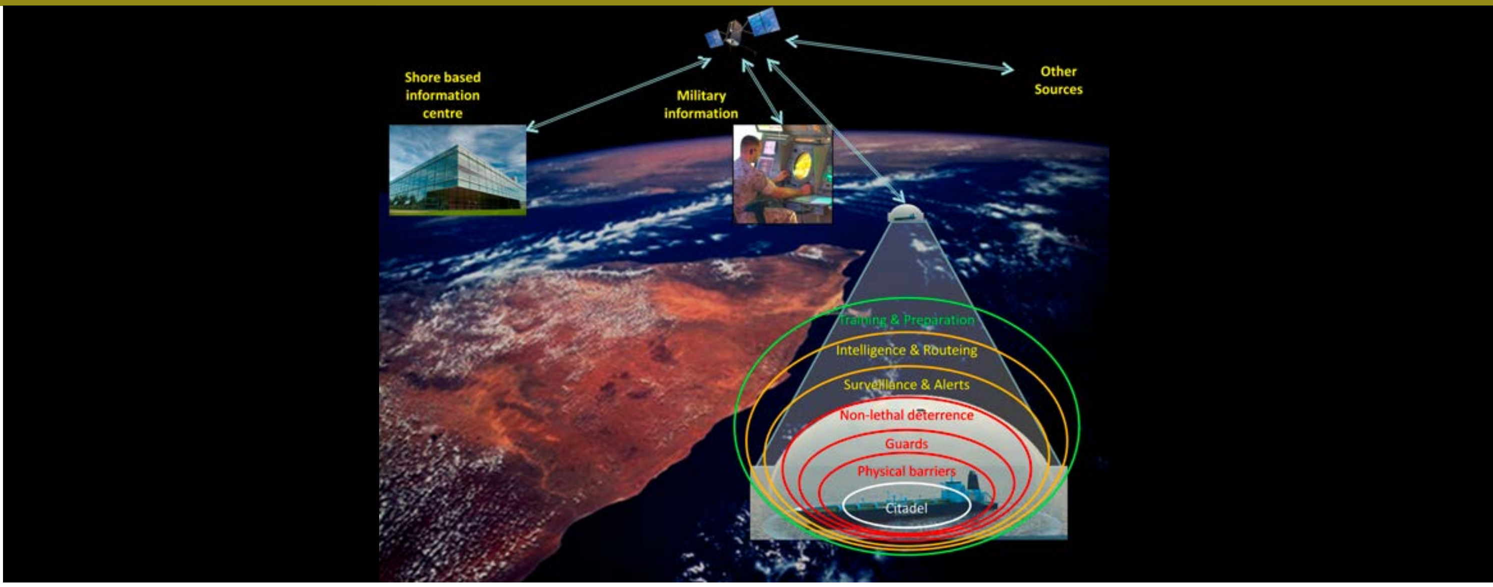
- literature and project reviews,
- end-user expert interviews,
- user surveys, and
- user workshops.

Results

The LOGSEC project delivered a roadmap for a large scale demonstration project in European logistics and supply chain security, characterised by adequate security for the benefit of business and governments, on low time-delay and other cost implications. LOGSEC identified the most relevant/promising research areas and research gaps, to be addressed in a possible follow-up demonstration project. An instrumental part of the roadmap project was to build a basis for future metrics necessary to evaluate supply chain and security performance and to monitor supply chain vulnerabilities.

PARTNERS	COUNTRY
EFP Consulting (UK) Ltd (EFPC)	United Kingdom
ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA (ATOS)	Spain
Cross-border Research Association (CBRA)	Switzerland
European Council of Transport Users (ESC)	Belgium
SZKOLA GLOWNA HANDLOWA W WARSZAWIE (POL)	Poland
Clecat - European Association for Forwarding, Transport, Logistics and Customs Service (CLECAT)	Belgium
Innovative Compliance Europe Ltd (ICE)	United Kingdom
Eidgenössische Zollverwaltung (SC)	Switzerland

PROMERC / Protection Measures for Merchant Ships



Information

Grant Agreement N°
607685
Total Cost
€3,131,452.00
EU Contribution
€2,224,958.00
Starting Date
01/03/2014
Duration
24 months

Coordinator

FLIR SYSTEMS LTD
(FLIR)
MARSS
2 Kings Hill Avenue
ME19 4AQ - West Malling -
United Kingdom
Contact
Craig Cooper
Tel: +44 1732 220011
E-mail:
Craig.Cooper@flir.uk.com
Website: www.flir.com

Project objectives

PROMERC aims to reduce the vulnerability of EU merchant fleets and maritime supply lines to criminal abduction and extortion and thereby reduce risk to mariners, shipping, and the environment, while also reducing costs. This will be delivered through the provision of:

» Independent review and recommendations about non-lethal technologies for pirate avoidance and opposing the boarding of vessels by pirates;

» An automated voyage planning support tool to aid shore based authorities, which will balance route management to mitigate risk against incurring additional fuel costs due to re-routeing and increased speed;

» An automated decision support tool to provide seafarers with real time threat assessment, evaluation of possible courses of action and a recommended course of action. A manual to aid in the selection and use of appropriate counter piracy measures in a layered holistic defence;

» Recommendations on the further development of counter piracy measures.

Description of the work

The PROMERC consortium brings together end-users, commercial, political, academic, and military entities along with leading research companies and agencies. The consortium's broad commercial and military security experience will be supported by active stakeholder engagement throughout.

The work falls into the following sections:

» Current and Future Non-Military Counter Measures

The first part of PROMERC will identify and catalogue the different existing and potential non military protection measures against piracy available to the shipping industry. In addition to identifying current and emerging measures, the catalogue will also differentiate between active versus passive measures. Within the active measures, differentiation will be made between lethal vs. non-lethal measures. An assessment of the operational effectiveness of the Counter-measures will be made.

» PEESLE constraints

An analysis of the Political-Economic-Ethical – Societal – Legal - Environmental (PEESLE) constraints on the use of existing and potential non-military protection measures will be performed.

» Evaluation of Options

The operational effectiveness and findings from the previous two work packages will be developed to conduct a total cost benefit analysis, to develop a manual to aid in the selection and use of appropriate counter piracy measures in layered holistic defence and a user configurable counter measures Knowledge base which will provide recommendations on counter measures based on user entered constraints, cost and effectiveness thresholds.

» Development of Tools

The heart of PROMERC will be the development and demonstration of decision aids for commercial shipping. One will provide an automated voyage planning support tool which will create seven day forecasts of piracy risks with real skill combining factors such as the day of the week, the moon phase and visibility, location, season, environmental conditions (e.g. wind speed), with ship and voyage specific factors to produce routes optimised to minimise cost and risk.

The other will be a Counter-Measures Decision Aid to provide dynamic situation sensitive advice and guidance to the bridge team incorporating near real time updates and underpinned by the Counter Measure Knowledge Base to produce accurate up-to-date assessments.

Expected results

The PROMERC project will apply advanced geospatial analysis and intelligence techniques to provide the shipping industry with a layered approach to planning, routeing and threat reduction that goes beyond current solutions. PROMERC will organize and consolidate the many dimensions of risk reduction by delivering a knowledge base, manuals and tools to assess the available counter-measures, the current and future threat situations, to identify and quantify the risks and to aid decisions before and during voyages. The system will provide situation and ship specific counter-measures and best practice guidance prior to and during the voyage, as well as interactive route planning tools to develop the counter-measures and sail plan to an acceptable level of risk and cost.

PARTNERS	COUNTRY
FLIR Systems Ltd (FLIR)	United Kingdom
NATO Science and Technology Organization (CMRE)	Italy
IMO World Maritime University (WMU)	Sweden
University of the Aegean – research Unit (UoA)	Greece
Security Association for the Maritime Industry Ltd (SAMI)	United Kingdom
Uniresearch B.V. (UNR)	The Netherlands
Netherlands Organisation for Applied Scientific Research (TNO)	The Netherlands
Engineering Ingegneria Informatica Spa (EII)	Italy
OLDENDORFF Carriers GmbH & Co KG (OLD)	Germany

SAFEPOST / Reuse and development of Security Knowledge assets for International Postal supply chains

© BMT GROUP LIMITED

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285104
Total Cost
€14,986,407.66
EU Contribution
€9,523,423
Starting Date
01/04/2012
End Date
31/03/2016

Coordinator

Association of European Public Postal Operators AISBL (PostEurop)
PostEurop Projects Department
114 Boulevard Brand Whitlock
1200 Brussels,
Belgium
Contact
Antonino Scribellito
Phone: +32 2 773 11 93
Mobile: +32 491 08 57 25
Fax: +32 2 771 48 58
E-mail:
antonino.scribellito@posteurop.org
Website:
www.posteurop.org
www.safepostproject.eu

Project objectives

SAFEPOST aims to raise the current level of postal security by integrating innovative screening solutions that: 1) do not disrupt the flow of enormous volumes of parcels and letters associated with operational postal processes and 2) support customs and counter-crime intelligence work within a European-wide cooperative distributed model.

Description of the work

Starting from the perspective of the partner postal operations, the project first identified the main security threats and threat actors and the main security gaps in postal operations. Secondly, it described security measures and process improvements to maintain or augment the efficient and secure operation of postal services to address the identified threats.

After completing an inventory of security gaps, this was developed into generic postal security models which were integrated into a Postal Security Target Operating Model. This enabled postal operators, customs and other relevant actors to understand how to securely exchange information related not only to security but also to the optimization of postal flows.

To support the Postal Security Target Operating Model, a Postal security platform was developed to help extend the current MEDICI effort. It exploited previous FP7 proect developments regarding e-freight and secure supply chains. SAFEPOST extended the concept of its Postal Security Target Operating Model to propose a ‘Common Postal Security Space’ with a view to creating a future European/World Postal Security information sharing system.

Results

» SAFEPOST saw strong interest from law enforcement agencies and custom authorities:

» A "Postal Security Forum" was created for the participation of all postal security supply chain stakeholders such as UPU; European Commission DGs TAXUD, MOVE, and HOME AFFAIRS; the WCO; and International Post Corporation (IPC) representatives so all could present the postal security technical challenges, latest developments and security projects of their respective organisations.

» A SAFEPOST work group was created to support the security and customs transversal aspects of PostEurop and to provide a common platform for PostEurop members to support the implementation of the project.

» A full-scale live demonstration of the SAFEPOST-based solutions was held to evaluate the feasibility and the benefits of the project's approach. The first demonstration took place at Iceland Post's sorting centre in Reykjavik on May 2015, to analyse the flow of postal items through D-Tube and to identify areas for improvements. A second live demonstration took place at Correos's sorting centre in June 2015 in Zaragoza, Spain. About 70 participants from DGs Home Affairs and TAXUD, PostEurop members, external supply chain stakeholders, customs authorities and SAFEPOST consortium partners attended the event, which underscored the improvements made since the first demonstration. Two more demos will take place in 2016.

PARTNERS	COUNTRY
Association of European Public Postal Operators AISBL (PostEurop)	Belgium
BMT Group Limited (BMT)	United Kingdom
Geopost – La Poste Group (GEO)	France
Totalförsvarets forskningsinstitut (FOI)	Sweden
Tellusecure AB (TLS)	Sweden
MJC2 Limited (MJC2)	United Kingdom
INLECOM Systems Ltd. (ILS)	United Kingdom
Correos y Telégrafos S.A. (COR)	Spain
Atos Spain S.A. (ATOS)	Spain
Stichting Nederlands Normalisatie-instituut (NEN)	The Netherlands
Confederation of Organisations in Road Transport Enforcement AISBL (CORTE)	Belgium
Hellenic Post S.A (ELTA)	Greece
K-NET S.A. (KNET)	Greece
MARLO AS (MARLO)	Norway
Fundación Zaragoza Logistics Center (ZLC)	Spain
CONCEPTIVITY (CPT)	Switzerland
Íslandspóstur hf (IP)	Iceland
Università degli Studi di Genova (UNIGE)	Italy
Cross-border Research Association (CBRA)	Switzerland
European Organisation for Security S.C.R.L. (EOS)	Belgium

ADABTS / Automatic detection of abnormal behaviour and threats in crowded spaces

© Lv Design - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218197
Total Cost
€4,483,794
EU Contribution
€3,229,034
Starting Date
01/08/2009
End Date
31/07/2013

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Division of Information Systems
Postal Box: 1165
SE-58111 Linköping
Sweden
Contact
Jörgen Ahlberg
Tel: +46 13378068
Mobile: +46 706757384
Fax: +46 13378287
E-mail:
adabts_coordinator@foi.se

Project objectives

ADABTS aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots by the automatic detection of threatening human behaviour.

ADABTS aims to develop models for threatening behaviours and algorithms for automatic detection of such behaviours as well as deviations from normal behaviour in surveillance data.

ADABTS aims to develop a real-time evaluation platform based on commercially available hardware, in order to enable high-performance, low-cost surveillance systems.

Description of the work

ADABTS will gather experts in human factors, signal processing, computer vision, and surveillance technology. In the first stage, focus will be on human factors in order to define and model behaviours. Then, the focus will be shifted towards automatic analysis of surveillance data (video and audio). Finally, a demonstration system will be implemented.

ADABTS will create models of behaviour that can be used to describe behaviours to be detected and how they can be observed. Such models will enable the prediction of the evolution of behaviour, so that potentially threatening behaviour can be detected as it unfolds, thus enabling pro-active surveillance. In order to detect behaviour defined by these models, advanced methods for sensor data analysis are needed. These methods should extract sensor data features that can be coupled with the defined behaviour primitives, and thus detect the presence of the (potentially) threatening behaviour.

ADABTS will develop new, and adapt existing sensor processing methods and algorithms for detecting and tracking people in complex environments, involving groups of people or crowds. Extracted sensor data features (e.g. tracks, voice pitches, body articulations) need to be related to the behaviour primitives, and, moreover, to be dynamic and to adapt to the context.

ADABTS will adapt the above algorithms to run on commercially available, low-cost hardware architectures consisting of multi-core CPUs combined with several multi-stream GPUs (Graphical Processing Units). Such hardware, in rapid development driven by the game industry, represents a huge potential for high-performance surveillance systems.

ADABTS will communicate results to the various kinds of identified actors: security stakeholders like European and national authorities, police organisations or event organizers; security system operators and security service companies; security system integrators; technology developers; the research communities for psychology and human factors; and signal processing communities.

ADABTS will involve all these actors, either as principal contractors, as subcontractors, or in an associated stakeholder group.

Results

Current automatic detection systems struggle to make inferences about the intent of human behaviour. ADABTS has addressed the problem of identifying threatening or anomalous behaviour by extracting characterizations in realistic security settings based on expert classifications and the analysis of operator behaviour. Furthermore ADABTS has developed models for certain threats (e.g., violence) and for the typical behaviour in specific contexts, as well as methods for detecting these threats and deviations from the typical behaviour in surveillance data. A prototype system has been developed, creating a proactive system that focuses on detecting the presence of threatening or anomalous behaviour. The system allowed for the operator to focus purely on suspicious situations, as opposed to trying to follow all situations at all times in public spaces.

ADABTS links different sensor techniques that allow for the system to cope with sensor uncertainties and thus enhancing the system performance. This allows for new system functionality that will disregard the vast amount of imagery that contains nothing unusual and will present events in the footage where something interesting might be going on. Improved events detection would benefit CCTV operators' effectiveness, leading to shorter reaction time concerning violent events. Furthermore, automated offline abilities, like searching databases, would also facilitate subsequent content-based retrieval in images after an incident. This creates new possibilities for increased security against threats like terror, crime and riots by enhanced warning systems. capabilities at a football stadium.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Stiftelsen SINTEF (SINTEF)	Norway
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Universiteit van Amsterdam (UvA)	The Netherlands
Institute of Psychology – Ministry of the Interior (IPMI)	Bulgaria
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Home Office Scientific Development Branch (HOSDB)	United Kingdom
Detec AS (Detec)	Norway

ARENA / Architecture for the recognition of threats to mobile assets using networks of multiple affordable sensors

© Kristian Peetz - Fotolia.com

Information

Grant Agreement N°
261658
Total Cost
€4,861,867.60
EU Contribution
€3,178,761
Starting Date
16/05/2011
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Swedish Defence
Research Agency
Gullfossgatan 6
STOCKHOLM, 164 90
Sweden
Contact
Åsa Waern
Tel: +46 13378084
E-mail: asa.waern@foi.se
Website:
http://www.foi.se

Project objectives

The objective of ARENA is to develop methods for automatic detection and recognition of threats, based on multisensory data analysis. Research objectives include:

» To robustly and autonomously detect threats to critical mobile assets in large unpredictable environments;

» To reduce the number and impact of false alarms and work towards optimized decision making;

» To demonstrate automatic threat detection for the land case (truck);

» To demonstrate an integrated, scalable and easy to deploy monitoring system;

» To assess automated threat detection for the land case (train) and the maritime case (vessel, oil rig);

» To evaluate detection performance and contribute to standards;

» To respect and respond to social, legal and ethical issues arising from the design, implementation and deployment.

Description of the work

ARENA addresses the design of a flexible surveillance system for detection and recognition of threats towards deployment on mobile critical assets/platforms such as trucks, trains, vessels, and oil rigs. There is a substantial end-user need for intelligent and continuous proactive monitoring to enable situational awareness and determination of potential threats enabling timely and appropriate response.

ARENA has a stakeholder group which consists of representatives from the land case and the maritime case.

The project will be carried out as an iterative systems development project. First, a threat analysis, development of user scenarios and user interaction will result in user requirements of the ARENA surveillance system for mobile platforms (WP2). The input will be used to develop the generic system architecture (WP3) and the different components necessary for the testbed (developed in WP4); the object assessment (WP5), the situation assessment (WP6), and the threat recognition (WP7). These components will to a large extent be developed in parallel, thus requiring much interaction between the work packages. The results from WP3, WP5, WP6 and WP7 (the latter including inputs from WP5 and WP6) are continuously integrated in the system testbed developed in WP4.

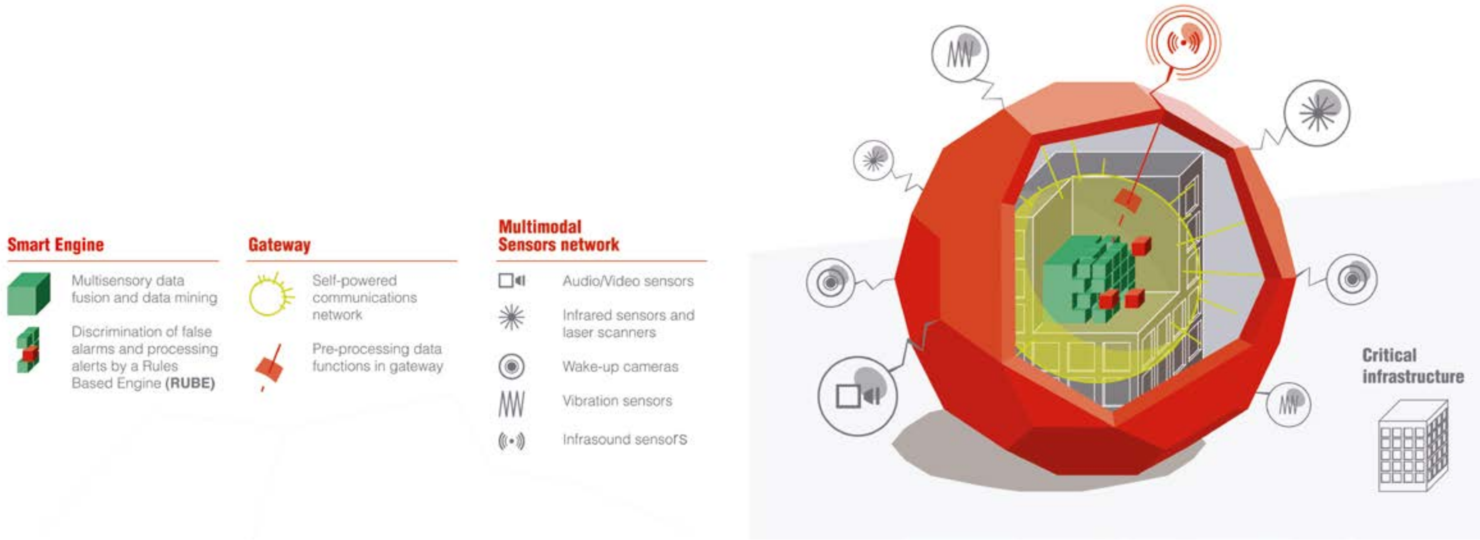
Once the testbed is completed, the remainder of the project deals with demonstrations and evaluations of the ARENA concept and system, providing experiences and feedback on the user requirements, the generic architecture, the different research areas related to the components and the testbed/system itself. Demonstrations will take place using the scenarios as developed in WP2, involving a truck case. Evaluation will be performed by means of testing and experimentation, using a thoroughly designed testing methodology. The Stakeholder Group will be involved throughout the Project.

Expected results

The expected result of ARENA is a system consisting of low cost sensors which are easy to deploy. The system will be adaptable to various platforms and increase the situation awareness.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
BMT GROUP LIMITED (BMT)	United Kingdom
ITTI Sp.zo.o. (ITTI)	Poland
SAGEM DEFENSE SECURITE (Sagem DS)	France
Morpho (MPH)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
THE UNIVERSITY OF READING (UoR)	United Kingdom
PRO DOMO SAS (PRODOMO)	France

ARGOS / Advanced pRotection of critical buildinGs by Overall anticipating System


Smart Engine
Multisensory data fusion and data mining
Discrimination of false alarms and processing alerts by a Rules Based Engine (RUBE)
Gateway
Self-powered communications network
Pre-processing data functions in gateway
Multimodal Sensors network
Audio/Video sensors
Infrared sensors and laser scanners
Wake-up cameras
Vibration sensors
Infrasound sensorS
Critical infrastructure

Information

Grant Agreement N°
313217
Total Cost
€4,645,416.00
EU Contribution
€3,464,258.50
Starting Date
01/01/2014
Duration
36 months

Coordinator

EVERIS SPAIN SL
Security & Defence
Avenida Manoteras 52
Madrid 28050 SPAIN
Contact
Mario Carabaño Marí
Tel: +34 91 749 00 00
E-mail: mario.carabano.mari@everis.com
Website: www.argos-project.eu

Project objectives

Socioeconomic activities such as supply and distribution of gas or electricity and the infrastructures that generate it or transport it are vital to the day-to-day functioning of any country. Due to several factors, the social and financial European situation, or supply constraints, energy and utilities have become a prominent issue in Europe.

Any uncontrolled disruption in those types of infrastructures may result in an unacceptable loss of human lives and a huge impact on the economic and social well-being of any country. It is critical to protect these infrastructures from threats to avoid potential disruption.

ARGOS [Advanced pRotection of critical buildinGs by Overall anticipating System] is a multimodal early warning security solution for Critical Infrastructures focused on low consumption technologies and detection algorithms based on data fusion and data mining smart techniques.

Description of the work

It is a 4.5 million euro project co-funded by the European Commission under the 7th Framework Programme that started in January 2014 and will end in December 2015. The ARGOS Consortium covers the entire value chain and includes all the expertise required for the successful execution of the project. The 13 partners are from seven different countries with a wide range of capabilities.

ARGOS will allow end-users to deploy the solution beyond the actual perimeter of the infrastructure, extending the "security zone" beyond the critical perimeter by defining wide early-warning areas that will enhance the Critical Infrastructures capacity to monitor, deter and respond to potential threats.

It is well-suited for remote semi-urban or non-urban environments where energy is not always available, since the solution will be based on an energy efficient algorithm for data processing, low-energy communications, self-powered networks of sensors, sleeping mode for video sensors and energy-efficient microelectronics. ARGOS will also focus on the development of non- privacy-invasive technologies such as vibration sensors and embedded video and audio analytics so capturing devices will transfer metadata instead of recorded images or sounds.

Some of the subsystems that encompass the ARGOS solution are, for example, vibration sensors, Infrared Cameras and Laser Telemeters, infrasound sensors, a module for data fusion and another one for data mining, audio and video analytics.

Expected Results

ARGOS will simultaneously evaluate and cross-check the inputs coming from the multimodal network of sensors in order to minimise false alarms, using data mining to account for correlations and interdependencies. Also the system will implement a "guided learning" methodology letting the operator teach the engine whether an alarm is true or false, in an iterative cycle of continuous and progressive improvement.

During the duration of the project, field trials will be done where the solution will be tested as means of validation. The first of the two trials will be done in Transgaz's facilities (Bucharest) and will test the protection of a long cross Critical Infrastructure, such as a gas pipeline. The second trial will take place in the nuclear facilities from the National Centre for Scientific Research Demokritos (Athens) and will test the protection of an energy producer critical infrastructure.

PARTNERS	COUNTRY
Everis (EVR)	Spain
S.C. Mira Telecom S.R.L. (MIT)	Romania
Aratos Technologies S.A. (ARA)	Greece
INFITHEON Technologies (INF)	Greece
Centre For Security Studies (KEMEA) (KEM)	Greece
HI-iberia Ingeniería y Proyectos (SL HIB)	Spain
Athens Information Technology (AIT)	Greece
VTT Technical Research Centre of Finland	Finland
Thales Services SAS (THA)	France
Charles University in Prague (CUNI)	Czech Republic
Athena GS3 Security Implementations Ltd (ATH)	Israel
National Centre for Scientific Research Demokritos (NCSRD)	Greece
Port Authority of Gijon (PAG)	Spain

BASYLIS / moBile, Autonomous and affordable SYstem to increase security in Large unpredIctable environmentS

© bluefern - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261786
Total Cost
€2,989,194.80
EU Contribution
€2,037,265
Starting Date
01/05/2011
End Date
31/05/2013

Coordinator

IP SISTEMAS
Calle Anabel Segura
nº 7- Planta B
28108, Alcobendas, Madrid
Spain
Contact
Sonia Gracia Anadón
Tel: +34 91 203 87 09
Mobile: +34 610 201 908
Fax: +34 91 209 78 28
E-mail: sgracia@indra.es
Website: www.basylis.european-project.eu

Project objectives

The BASYLIS system aims to create a transportable security platform capable of detecting a wide range of predetermined security threats.

The prototype design will include five highly sensitive sensors exploiting different parts of the spectrum: radio, magnetic, seismic, acoustic and optical waves, as well as images via intelligent video.

Description of the work

The principal obstacles to early threat detection in wide areas are of two types: functional (e.g. false-alarm rate) and ethical (e.g. privacy). Both problems are exacerbated when either the installations or the environments are dynamic.

The information gathered by these sensors is brought together into an information layer composed of three levels: multi-sensor integration (MSI), image processing and risk assessment.

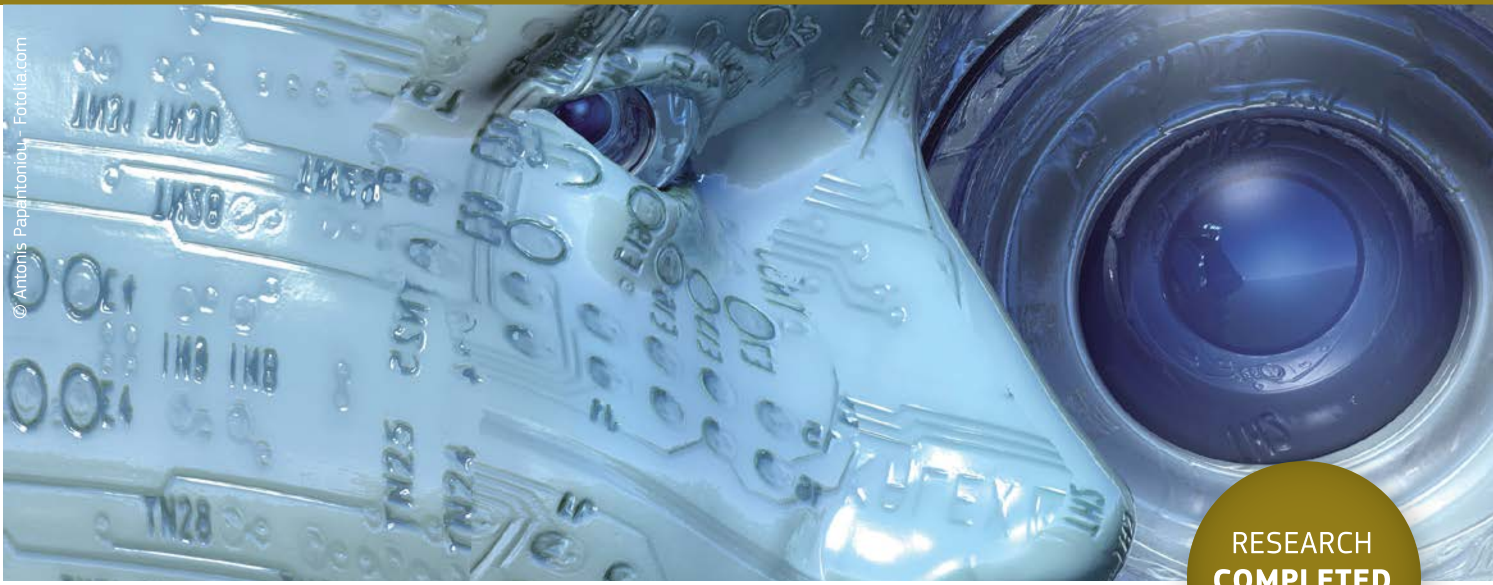
The BASYLIS system integrates all the sensors in a unified system, incorporating three intelligence levels and merges alarms coming from different sensor for the same object before sending the data to a Behavioural Analysis module.

Results

A system that ensures the complete protection of a Refugee camp on different levels thanks to long range systems like radar and ladar, to low range systems like underground seismic and metal sensor, and personal protection systems like bracelets and button alarm system, all with the aid of a system of video classification and an Acoustic Vector Sensors system and a multi-tracker and behaviour analysis system.

PARTNERS	COUNTRY
IP SISTEMAS (IP)	Spain
NEW TECHNOLOGIES GLOBAL SYSTEMS (NTGS)	Spain
UNIVERSITA DEGLI STUDI DI FIRENZE (UFL)	Italy
TERMA A/S (TERMA)	Denmark
MICROFLOWN (MICROFLOWN)	The Netherlands
MIRASYS OY (MIRASYS)	Finland
UNIVERSIDAD POLITECNICA DE MADRID (UPM)	Spain
UNIVERSITY COLLEGUE LONDON (UCL)	United Kingdom
CENTRO NACIONAL DE PROTECIÓN DE INFRAESTRUCTURAS (CNPIC)	Spain

IDETECT 4ALL / Novel Intruder Detection & Authentication Optical Sensing Technology



© Antonis Papantoniou - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217872
Total Cost
€3,239,571
EU Contribution
€2,298,014
Starting Date
01/07/2008
End Date
30/06/2011

Coordinator

INSTRO PRECISION LTD.
15 Hornet Close
Pysons Rd Industrial Estate
Broadstairs, Kent, CT10 2YD
United Kingdom
Contact
William Caplan, MSE
Electro-optic Project Manager
Instro Precision Limited.
Tel: +44 (0) 1843 60 44 55
ext. 110
E-mail:
williamcaplan@instro.com
Website:
www.idetect4all.com

Project objectives

This project's overarching objective was to develop and test a system of sensor technologies to protect critical infrastructure. A key driver was to find ways to overcome the high cost and unacceptable false alarm rates that limit the deployment of existing security sensor technologies.

Much of iDETECT4ALL's work focused on prototype sensors to detect intruders and remotely scan/read optical tags worn by authorised personnel and vehicles. A system architecture was defined to capture sensor alert event data, transmit this to a remote control centre and enable an imaging system to view the intruder event.

Work was divided into the following phases:

» review of end user requirements;

» system architecture definition;

» technology R&D until the prototype design and manufacture stage;

» system integration;

» field trials;

» analysis and evaluation.

Results

After consultations with end-users, the consortium developed a technological system consisting of:

» a low-cost prototype communication network to transmit event messages;

» a "back-office" database linked to control centre application software;

» a geographic information system (GIS) to correlate with alerts;

» a high resolution imaging system based on an internet control protocol to accept sensor alerts and pivot to view the event detected.

These elements were integrated and then tested in field experiments at airports in Portugal (Faro) and Belgium (Liege) using representative critical infrastructure protection scenarios. A wide variety of test cases were examined, including authentication and detection of walking and running personnel, and moving vehicles. The 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 their system delivered useful levels of real world performance, while confirming that the project's objectives of achieving a very low false alarm rate and high detection rates were achieved. A key technological breakthrough was made with the development and successful testing of a single sensor able to both detect intruders and also authenticate personnel and vehicles by reading remote optical tags.

Though the project consortium said there is scope for further improvement of the sensor performance through additional optimisation of the hardware and signal processing algorithms, it argues that there is a good market opportunity to materialise and exploit the know-how gained in the project via a number of products.

According to the project's research partners, suitable levels of investment in optimisation and engineering for production in iDETECT4ALL's sensor and associated system could lead to "improved protection for critical infrastructures in the European Union and the world."

PARTNERS	COUNTRY
Instro Precision Ltd.	United Kingdom
Motorola Israel Ltd.	Israel
EVERIS Consulting	Spain
Cargo Airlines	Israel
3D s.a.	Greece
ANA Aeroportos de Portugal	Portugal
LACHS	Belgium
Azimuth Tecnologies Ltd.	Israel
S.C. PRO OPTICA S.A.	Romania
Halevi Dweck & Co. Arttic Israel Company Ltd. (ARTTIC)	Israel
Arttic Israel International Management Services 2009 Ltd (AIL)	Israel

INDECT / Intelligent information system supporting observation, searching and detection for security of citizens in urban environment

© Auke Holwerda - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218086
Total Cost
€14,984,466
EU Contribution
€10,906,984
Starting Date
01/01/2009
End Date
30/06/2014

Coordinator

AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY
Department
of Telecommunications
Al. A. Mickiewicza 30
PL-30059 Kraków, Poland
Contact
Prof. Andrzej Dziech
Tel: +48 12 6172616
Mobile: +48 607 720 845
Fax: +48 12 6342372
E-mail: dziech@kt.agh.edu.pl
Website:
www.indect-project.eu/

Project objectives

The **main objectives** of the INDECT Project were:

» to develop an intelligent information system for automatic detection of threats and recognition of criminal behaviour or violence;

» to develop new methods and techniques providing tools to support activities of police officers, including tools for threat detection on the Internet; this included the development of a new type of search engine combining direct search of images and video based on watermarked contents and storage of metadata in the form of digital watermarks;

» to develop techniques for data and privacy protection in storage and transmission of data based on quantum cryptography and new methods of digital watermarking.

Description of the work

The INDECT Project aimed to develop tools for enhancing the security of citizens and protecting the confidentiality of recorded and stored information as well as the privacy of involved persons. INDECT targeted threat detection in both real environments (intelligent cameras) and virtual environments (computer networks, especially Internet).

The INDECT methodology addressed, firstly, the detection of specific crimes (such as Internet child pornography, trafficking of human organs, spread of botnets, viruses, malware as well as terrorism, and organised crime), then the detection of the source of the identified crimes (for example, specific criminals responsible for the crimes). It is always a human being (police, security services, etc.) who ultimately decides whether an intervention should take place once a source has been identified.

It should be underlined that the INDECT project was a research project, allowing involved European scientists to develop new, advanced and innovative algorithms and methods aimed at combating terrorism and other criminal activities, such as human trafficking and organised crime, which are affecting citizens' safety.

The INDECT Project ensured strict fulfilment of the EU ethical regulations on privacy, data protection, prevention of dual use, etc. In accordance with these regulations, a great deal of attention was paid to ethical issues, and among others, the INDECT Project never involved processing of any personal data without the prior written consent of individuals.

Results

The INDECT project ("Intelligent information system supporting observation, searching and detection for security of citizens in urban environment", http://www.indect-project.eu/) worked on developing solutions designed for police and other law enforcement authorities in the EU. Focusing on automatic threat detection in urban environments, the project team developed a set of tools supporting decision-making in counteracting threats and criminal activities.

European scientists and researchers developed solutions and tools for automatic threat detection. The primary objective was to develop advanced and innovative algorithms for human decision support in combating terrorism and other criminal activities, such as human trafficking, child pornography, detection of dangerous situations (e.g. robberies), and the use of dangerous objects (e.g. knives or guns) in public spaces.

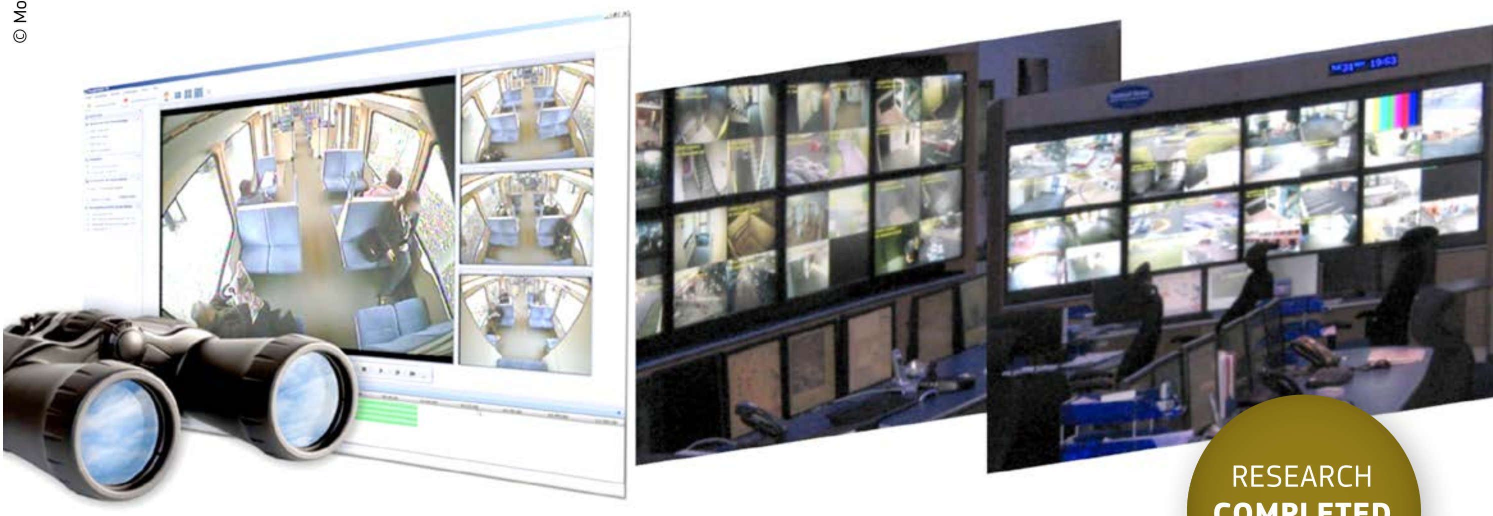
A significant part of the project was dedicated to the development of tools and methods for data and privacy protection. The processed information is protected before its transmission or storage to prevent any attempts at unauthorised access. Dedicated tools have been developed to protect citizens' privacy in areas covered by visual monitoring systems.

The main tangible INDECT results are over 50 working prototypes. Some of them were presented and awarded at international exhibitions and conferences.

PARTNERS	COUNTRY
AGH University of Science and Technology (AGH)	Poland
APERTUS Távoktatás-fejlesztési Módszertani Központ Tanácsadó és Szolgáltató Közhasznú Társaság (APERTUS)	Hungary
Gdansk University of Technology (GUT)	Poland
InnoTec DATA G.m.b.H. & Co. KG (INNOTEC)	Germany
Grenoble INP (INP)	France
General Headquarters of Police (GHP)	Poland
INDESOL (INDESOL)	Spain
PSI Transcom GmbH (PSI)	Germany
Police Service of Northern Ireland (PSNI)	United Kingdom
Poznan University of Technology (PUT)	Poland
Universidad Carlos III de Madrid (UC3M)	Spain
Technical University of Sofia (TU-SOFIA)	Bulgaria
University of Wuppertal (BUW)	Germany
University of York (UoY)	United Kingdom
Technical University of Ostrava (VSB)	Czech Republic
Technical University of Kosice (TUKE)	Slovakia
X-Art Pro Division G.m.b.H. (X-ART)	Austria
Fachhochschule Technikum Wien (FHTW)	Austria

MOSAIC / Multi-Modal Situation Assessment & Analytics Platform

© Mosaic



RESEARCH **COMPLETED**

Information

Grant Agreement N°
261776
Total Cost
€3,606,642
EU Contribution
€2,664,559
Starting Date
01/04/2011
End Date
31/07/2014

Coordinator

THE UNIVERSITY OF READING
Intelligent Media Systems and Services Research Laboratory, School of Systems Engineering
Whiteknights Campus
PO Box 217
RG66AH Reading,
United Kingdom
Contact
Prof. Atta Badii
Tel: +44 (0) 118 378 7842
Fax: +44 (0) 118 975 1994
E-mail:
atta.badii@readiing.ac.uk
Website:
www.imss.reading.ac.uk

Project objectives

MOSAIC developed and validated:

» A framework for capturing and interpreting the use-context requirements underpinned by a standard data ontology to facilitate the tagging, search and fusion of data from distributed multimedia sensors, sources and databases;

» A systems architecture to support wide area surveillance with edge and central fusion and decision support capabilities;

» Algorithms, including hardware-accelerated algorithms for smart cameras, which enable disparate multi-media information correlation to form a common operating picture, including representation of the temporal information and aspects;

» Tools and techniques for the extraction of key information from video, uncontrolled text and databases using pattern recognition and behaviour modelling techniques;

» Algorithms and techniques to represent decisions and actions within a mathematical framework, and how this framework can be used to simulate the effects of disturbances on the system.

Description of the work

MOSAIC Platform involved multi-modal data intelligence capture and analytics including video and text collaterals etc. The distributed intelligence within the platform enabled decision support for automated detection, recognition, geo-location and mapping, including intelligent decision support at various levels to enhance situation awareness, surveillance targeting and camera handover; these involved level one fusion, and situation understanding to enable decision support and impact analysis at level two and three of situation assessment. Accordingly MOSAIC developed and validated: i) A framework for capturing and interpreting the use-context requirements underpinned by a standard data ontology to facilitate the tagging, search and fusion of data from distributed multi-media sensors, sources and databases, ii) A systems architecture to support wide area surveillance with edge and central fusion and decision support capabilities, iii) Algorithms, including hardware-accelerated ones for smart cameras, which enable disparate multi-media information correlation to form a common operating picture, including representation of the temporal information and aspects, iv) Tools and techniques for the extraction of key information from video, un-controlled text and databases using pattern recognition and behaviour modelling techniques, v) Algorithms and techniques to represent decisions and actions within a mathematical framework, and how this framework can be used to simulate the effects of disturbances on the system, vi) An integrated system solution based upon the proposed systems architecture and the above developed enabling technologies including techniques for tagging different multi-media types with descriptive metadata to support multi-level fusion and correlation of surveillance and other data intelligence from distributed heterogeneous sources and networks.

Results

MOSAIC project delivered a significant number of modules and components for decision supported targeted surveillance as integrated into the MOSAIC Demonstrator Framework.

These are:

1) Semantic Representation Framework & Data Model
2) Ontology-Based Reasoning
3) Decision Support System
4) The Template Matching Decision Support (TMDS)
5) Data/Text Mining Component
6) Social/Criminal Network Analysis Tools
7) Automatic Generation and Prioritisation of Networks
8) Smart Camera Component Single & Multi-Camera Tracking
9) Person/Group Detection & Tracking
10) Optical Flow based Crowd Motion Analysis
11) Detection of Loitering Mugging, People Carrying Large Objects, and, Left-behind Objects
12) VIKI The VIKI (View It, Know It)

MOSAIC innovations have had a major impact on bandwidth economies for security surveillance systems at various levels. For example, network traffic efficiency: the ability to pre-process events on the camera itself enabling a more focused and targeted surveillance. This is driving several other benefits such as lower storage requirements, adaptability, easier installation and maintenance, reduced overall costs and better targeting of surveillance resources. The MOSAIC domain model is generic enough to facilitate easy adaptation to domains where a media-independent representation of a wide range of real-world situations and events is needed.

PARTNERS	COUNTRY
The University of Reading (UoR)	United Kingdom
BAE Systems (Operations) Ltd (BAE)	United Kingdom
A E Solutions (BI) (AES)	United Kingdom
SYNTHEMA S.R.L. (SY)	Italy
TECHNISCHE UNIVERSITAT BERLIN (TUB)	Germany
DResearch Digital Media Systems GmbH (DR)	Germany
WEST MIDLANDS POLICE AUTHORITY (WMP)	United Kingdom
INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)	Belgium
WARWICKSHIRE POLICE (WP)	United Kingdom

P5 / Privacy Preserving Perimeter Protection Project

Information

Grant Agreement N°
312784
Total Cost
€4,823,592.80
EU Contribution
€3,499,169.00
Starting Date
01/08/2014
Duration
36 months

Coordinator

FOI – TOTALFORSVARETS FORSKNINGSINSTITUT
Division of Sensor
and EW Systems
Olaus Magnus väg 42
Linköping 581 11
SWEDEN
Contact
Dr. Ola Friman
E-mail: ola.friman@foi.se

Project objectives

The goal of P5 is the development of an intelligent, proactive perimeter surveillance system that works robustly under a wide range of weather and lighting conditions and that has strong privacy preserving features. The system will monitor the region outside the security area of critical buildings and infrastructure, and give early warning if terrestrial or airborne threats are detected. The work is carried out by nine partners and is coordinated by FOI, the Swedish Defence Research Agency. The research and development activities within P5 are financed by the participating organisations themselves and by the European Commission through the Framework 7 Grant 312 784.

Description of the work

The system will support, rather than replace, a human operator. A low false alarm rate due to animals or other innocuous events, combined with high threat detection sensitivity and privacy standards, are central ambitions of the project. To achieve these goals, a multispectral sensor suite comprising both passive and active sensors is envisaged, i.e., a system based on radar, visual and thermal sensors. The sensor suite will be complemented with advanced algorithms for information fusion, object detection and classification, privacy preservation, and high level modelling of intent and behaviour analysis.

Expected results

The P5 project is strongly user-driven and demonstration of the developed surveillance system will be conducted at two different critical infrastructure sites. Finally, the P5 project will make contributions to evolving standards in detection systems.

PARTNERS	COUNTRY
TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)	Sweden
THE UNIVERSITY OF READING (UOR)	United Kingdom
TERMISK SYSTEMTEKNIK I SVERIGE AB (TST)	Sweden
SAGEM DEFENSE SECURITE (SAG)	France
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX DE NAMUR (FUNDP)	Belgium
VISUAL TOOLS SA (VT)	Spain
IMST GMBH (IMST)	Germany
OKG AKTIEBOLAG (OKG)	Sweden
HOME OFFICE CAST	United Kingdom

SAMURAI / Suspicious and Abnormal behaviour Monitoring Using a netwoRk of cAmeras for sItuation awareness enhancement

© diego cervo - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217899
Total Cost
€3,723,071.40
EU Contribution
€2,478,051.50
Starting Date
01/06/2008
End Date
30/11/2011

Coordinator

QUEEN MARY,
UNIVERSITY OF LONDON
Department of Computer
Science
Mile End Road
E1 4NS London
United Kingdom
Contact
Shaogang GONG
Tel: +44 20 7882 5249
Fax: +44 20 8980 6533
E-mail: sgg@dcs.qmul.ac.uk
Website:
www.samurai-eu.org

Project objectives

The aim of SAMURAI was to develop and integrate an innovative surveillance system for monitoring both the interior and surrounding areas of a critical public infrastructure site.

The project set out to achieve three key innovations:

» combining networked sensors, rather than isolated visual sensors (e.g. standalone CCTV cameras), so that multiple complementary sources of information are fused in order to obtain a complete surveillance picture;

» developing intelligent video analytics, as well as an online adaptive behaviour monitoring system, for real-time abnormal behaviour detection;

» integrating fixed-position CCTV video footage with mobile sensory input from patrolling staff for more effective "man-in-the-loop" decision-making back at the operations centre.

Results

SAMURAI produced a range of new operating concepts, software and hardware to achieve its scientific research goals.

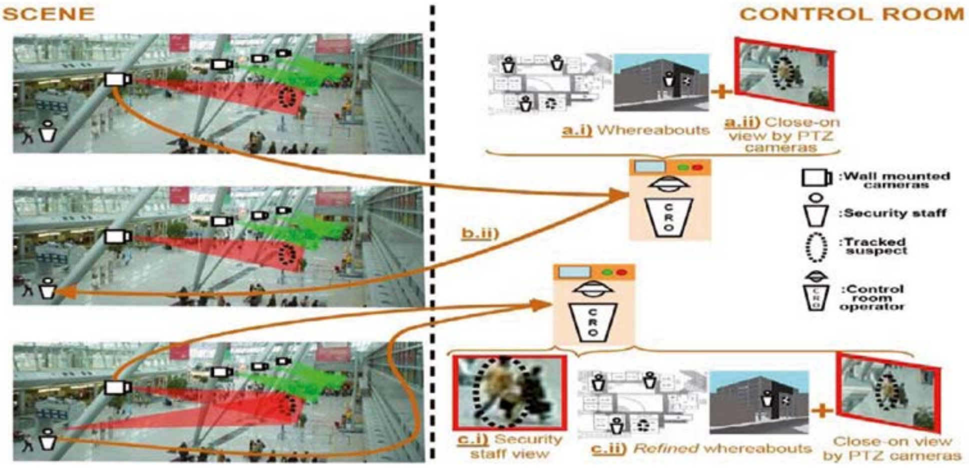
For combining sensor data, SAMURAI produced new visualisation software, the SUMURAI GUI, to display data from different inputs in one window. As well as active 3D image mapping, this includes a background algorithm that automatically filters out "useless" motion from sensor images to leave only relevant, "action needed" highlights.

For abnormal behaviour detection, the project combined multi-sensor source data processing with a series of pre-programmed abnormal, rare or "of interest" behavioural triggers. Data points such as audio abnormalities, obvious attempts to conceal one's identity, or movements against the regular "flow" of crowded area traffic are fed into this system to produce "focus of attention" (FoA) prioritisation for operators.

Finally, to integrate sensory input from patrolling staff, SAMURAI designed and developed the Ninja, a wearable sensor suit with built in data ports for camera and audio inputs. Supported by a wifi-based remote processing unit known as the BPS Ngine system, the project produced 50 operating Ninja units. Each unit can augment fixed position sensors by giving operators an "eyes on target" update to other feeds.

When combined, the results produced by SAMURAI represent a highly integrated and advanced situational awareness system. The use of data fusion algorithms throughout ensures that the SAMURAI system displays only the most pertinent data and knowledge regarding the current situation.

In addition it allows the end-user to alter their awareness picture in real-time, to support almost immediate staff prioritisation during a security incident.



© Samurai

PARTNERS	COUNTRY
Queen Mary, University of London	United Kingdom
Università degli Studi di Verona	Italy
Elsag Datamat S.p.A.	Italy
Waterfall Solutions Ltd	United Kingdom
Borthwick-Pignon OÜ	Estonia
Esaprojekt SP. Z O.O.	Poland
Syndicat Mixte des Transports pour le Rhône et l’Agglomération Lyonnaise	France
BAA Limited	United Kingdom

SUBITO / The Surveillance of Unattended Baggage and the Identification and Tracking of the Owner

© Artsem Martysiuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218004
Total Cost
€3,897,587.20
EU Contribution
€2,581,052,60
Starting Date
01/01/2009
End Date
31/10/2011

Coordinator

SELEX SENSORS AND AIRBORNE SYSTEMS LIMITED
2 Crewe Road North
Edinburgh - EH5 2XS
Scotland
United Kingdom
Contact
Ms Georgette Murray
Mark Riddell
Tel: +44 (0) 131 343 5992
Fax: +44 (0) 131 343 8110
E-mail: mark.riddell@selex-galileo.com
Website:
www.subito-project.eu

Project objectives

SUBITO set out to further develop new technologies for processing visual images and applying threat assessment algorithms for identifying baggage lost by individuals in a crowded public space. The overall objective of the project was to remotely facilitate the:

» fast detection of baggage that has been abandoned;

» fast identification of the individual who left the baggage;

» fast determination of their current location, or path they followed.

© illushooti - Fotolia.com

Results

SUBITO developed its system architecture in the context of existing lost baggage procedures used by stakeholders. It also applied an ethical review related to privacy requirements in EU law, and produced background material on the wider social and legal aspects of visual monitoring technology.

The eventual defined system required novel advancements for visual processing camera technology and for the distributed processing of threat assessment data. These were:

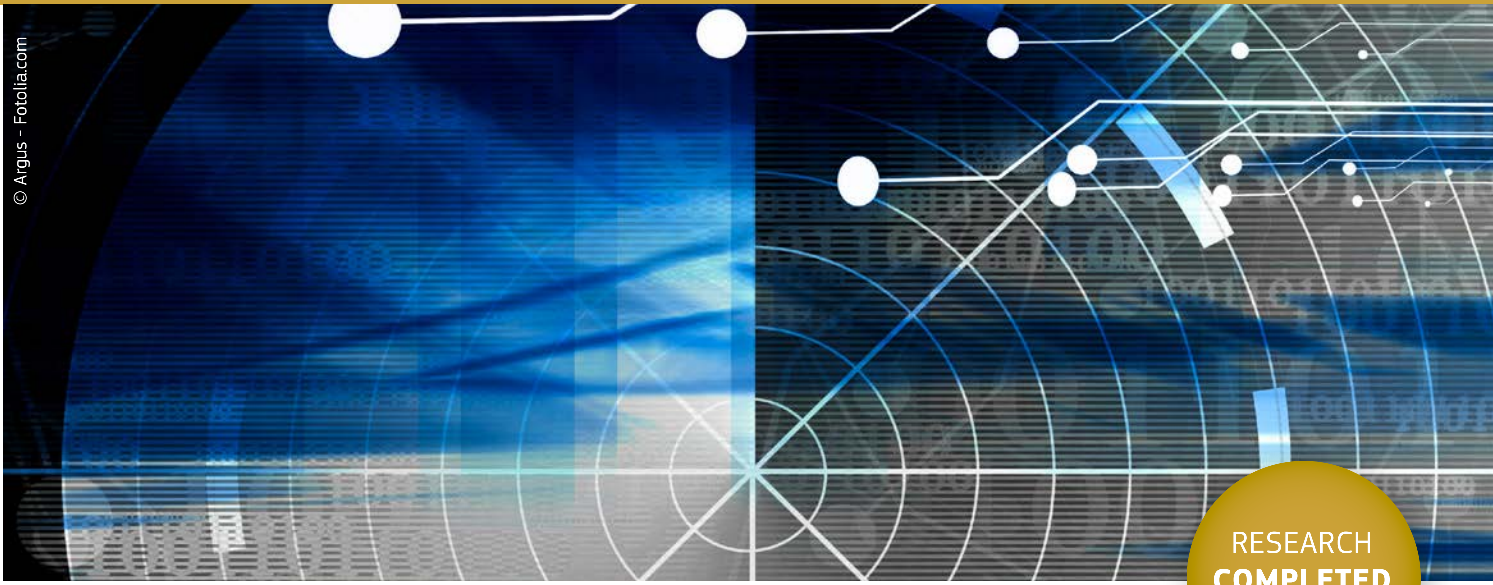
» Visual: image analysis algorithms were combined with improved camera technology to enhance the ability to detect, segment, track and classify moving objects within a scene. This was achieved by using a multi-view approach, which reduced the system's false alarms;

» Threat assessment: processing algorithms were developed to better classify potentially critical situations, by giving positional and classification data about the objects and people within the sensed environment. Research indicates that the inclusion of reasoning about the intentions of individuals within a scene, and the interactions between these individuals, leads to greatly improved performance of the state of the art. In particular, the SUBITO system exceeds the processing achievements of the previous ISCAPS study.

The project culminated in the final demonstration and evaluation of an integrated system, operating in pre-recorded scenarios. The demonstration illustrates advances towards the overall objectives mentioned above.

PARTNERS	COUNTRY
SELEX Sensors and Airborne Systems Limited	United Kingdom
ELSAG DATAMAT S.p.A	Italy
Office National d'Etudes et de Recherches Aérospatiales	France
L-1 Identity Solutions AG	Germany
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
University of Leeds	United Kingdom
University of Reading	United Kingdom
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Österreicheshes Forschungs und Prufzentrum Arsenal Ges.m.bH	Austria
Fiera di Genova S.p.A	Italy
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom

ARGUS 3D / AiR GUidance and Surveillance 3D



© Argus - Fotolia.com

RESEARCH COMPLETED

Information

Grant Agreement N°
218041
Total Cost
€4,943,520
EU Contribution
€3,262,050
Starting Date
01/12/2009
End date
30/11/2012

Coordinator

SELEX SISTEMI INTEGRATI SPA
Civil Systems Business Unit
Via Tiburtina, 1231
00131 Rome
Italy
Contact
Claudia Fusai
Tel: +39 06 4150 5370
Fax: + 39 06 4150 2043
E-mail: cfusai@selex-si.com
Website:
http://www.argus3d.eu/

Project objectives

The overall objective of the ARGUS 3D project is to enhance the security of European citizens, as well as of strategic assets by contrasting, over large areas, unpredictable and unexpected terrorist threats that can be delivered by means of small and low-flying (manned or unmanned) aircraft.

In order to achieve this general objective, the project intends to carry out R&D activities aimed at improving the current ATC systems for civil applications, extending their coverage and making them able to detect, recognise and track non-cooperative targets.

The scientific and technical objective of the ARGUS 3D project is studying, designing and implementing an innovative, low-cost, multi-sensor, radar-based system for 3D air guidance and surveillance (the "ARGUS 3D" system) that integrates conventional surveillance systems currently used for civil applications and two classes of non-conventional radar systems: 3D PSR sensors and networks of multi-operational passive/bistatic radar sensors.

Description of the work

The ARGUS 3D project aims at studying, designing and implementing two types of non conventional radar systems:

» The 3D PSR, a solution that, using a monopulse approach which exploits the difference of the gain of two radar beams of a conventional multi-beam 2D PSR, allows for obtaining an estimation of the aircraft altitude;

» The Passive/Bistatic radars, special forms of radar systems that, rather than emitting pulses, rely on sources of illumination already available in the environment to illuminate potential targets and are able to detect and track objects by analysing the way these objects reflect the signals coming from the transmitters of opportunity.

The ARGUS 3D system functionalities will take into account information provided by innovative 3D PSRs and passive radar networks, processing and merging them with existing radar data, thus exploiting and enhancing the performances and capabilities with respect to conventional surveillance and ATC systems.

The presence of new sensors, with respect to conventional ATC systems, and the final goal of the project (the security enhancement) requires the development of:

» a Consistency function to compare the data from the different sensors and check their integrity;

» a Decision Support function to distinguish between cooperative and non-cooperative air traffic, thus providing a warning every time a risk of terrorist attack occurs and suggesting to the operators the right actions;

» a new Data Presentation function to show, in a dedicated display, further information in addition to conventional air traffic information.

The project includes:

» a controlled demonstration in a real environment of the feasibility of the ARGUS 3D approach and the improvement of ATC security, checking the detectability of low flying small-RCS air vehicles (using the passive radar) and the ability to evaluate the altitude of non cooperative vehicles (using only PSR 3D);

» an evaluation, in a simulated environment, of the overall ARGUS 3D integrated system.

Results

ARGUS 3D developed two types of non-conventional radar systems that can detect, recognize and track NCT (non-cooperative targets). The first system, "3D PSR", uses a monopulse estimation capability in the vertical plane, enabling it to identify the altitude of any detected target. The second system – composed of passive and bi-static radar sensors – detects and tracks objects by processing reflections from sources of illumination already available in the environment such as commercial broadcasts or communication signals.

The two systems were successfully tested in seven different scenarios:

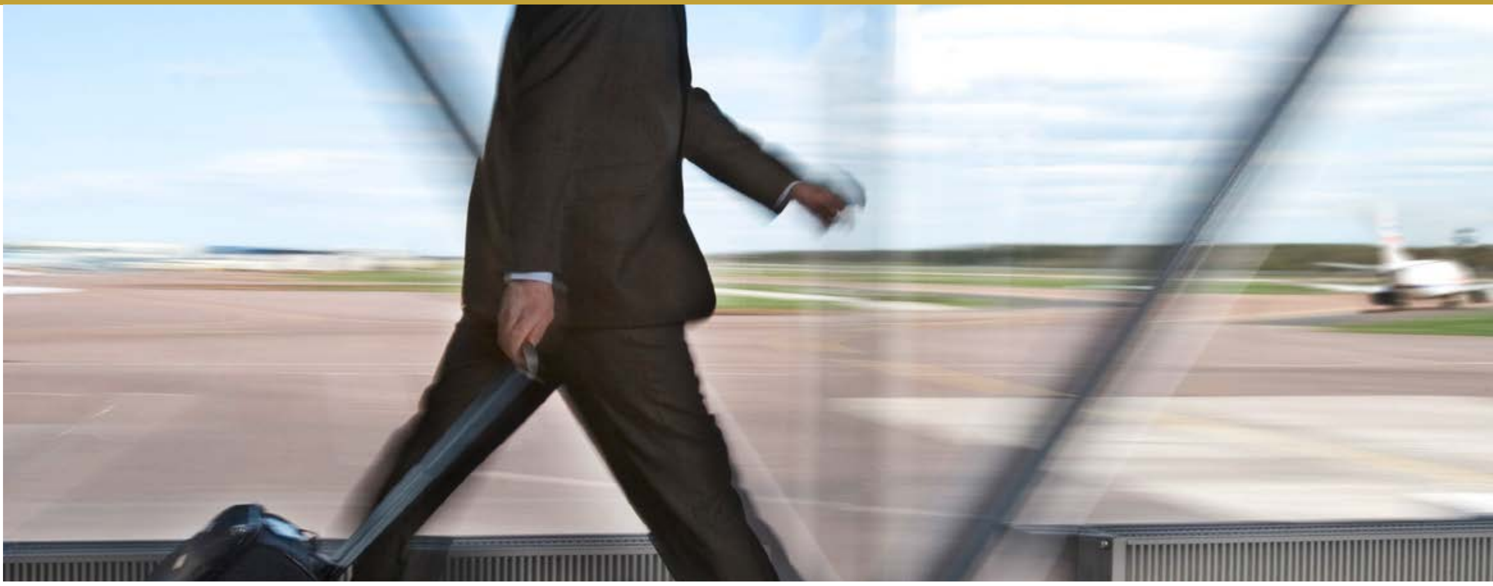
1. small civil airport
2. transponder out of service or switched off
3. tracking of ultra-light motorized
4. small touristic aircraft
5. commercial flights
6. PSR (primary surveillance radar) out of service
7. quasi-real simulated scenario (Rome region)

In each test, ARGUS 3D systems were tested alongside conventional ATC systems. All the results obtained confirmed that ARGUS 3D could improve current ATC systems via :

- • extending the coverage for specific zones where conventional systems typically have difficulty
- greater provision of estimated altitude of targets where this was previously impossible
- passive radar networks to fuse information and alarm systems
- provision of surveillance information without interruption
- control of the flight in case of data provided by conventional surveillance
- updating of the final user about the dangerous situation detected by the passive radar network
- establishing a suitable security level and reaction time upon detection of a target

PARTNERS	COUNTRY
Selex Sistemi Integrati (SELEX-SI)	Italy
SESM Scarl (SESM)	Italy
Università "La Sapienza" di Roma Dip. di Scienza e Tecnica dell'Informazione e della Comunicazione (INFOCOM)	Italy
Przemysłowy Instytut Telekomunikacji S.A. (PIT)	Poland
University College of London (UCL)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
ENAV S.p.A (ENAV)	Italy
ECONET S.L. (ECONET)	Spain
Dependable Real Time Systems Ltd. (DRTS)	United Kingdom
ISO Software Systeme GmbH (ISO)	Germany
REDHADA S.L. (REDHADA)	Spain
CiaoTech Srl (CTECH)	Italy

ABC4EU / Automated Border Gates For Europe



Information

Grant Agreement N°
312797
Total Cost
€16,817,103.60
EU Contribution
€12,015,246.04
Starting Date
01/01/2014
Duration
42 months

Coordinator

INDRA SISTEMAS S.A. (INDRA)
SECURITY SYSTEMS / ELECTRONIC IDENTITY
ANABEL SEGURA 7
28108 – Alcobendas-Madrid - Spain
Contact
Daniel Cuesta
Tel: +34 91 480 7993
Fax: +34 628 23 82 50
Fax: +34 91 480 6031
E-mail: dcuesta@indra.es
Website: www.abc4eu.com / www.abc4eu.eu

Project objectives

The Main Goals of the ABC4EU Project are:

» Analyse the ABC concept vs EU legislation, in particular the Schengen Border Code, to identify which processes can / cannot be automated and the impact that different levels of automation could have in the SBC procedures.

» Optimize and harmonize the ABC processes related to the increasing flow of people crossing borders.

» Assess the feasibility of a future Registered Travel Programme (RTP) in the EU which could be integrated into the ABC gates that would allow third country nationals to benefit from an automated BCP process in terms of flow efficiency, while maintaining the security requirements of the border crossing.

» Assess the feasibility of a future Entry / Exit System (EES) in the EU which could be integrated into the ABC gates.

» Evaluate, optimize and harmonize the use of 2nd generation passports biometrics for passengers' identification.

» Identification and design of a basic set of features to achieve a common user experience.

» Identification and removal of obstacles which are preventing today the certification distribution throughout Europe both for ePassport verification (CSCA – DS certificates) and for Extended Access Control (TA certificates) to access the fingerprint information in 2nd generation ePassports.

» Assess and evaluate the compliances of the proposed processes with the legal requirements to protect fundamental rights, in particular the protection of personal data and with ethical principles.

Description of the work

The main objective of the ABC4EU project is to update and integrate the current ABC gates systems already deployed in many member states extending its use to second generation passports and citizens of countries outside the EU. In ABC4EU, the upgrade and testing of the ABC gates will be done in the pilots deployed in Spain and Portugal (in airports, harbours and land borders).

In ABC4EU, RTP and EES concepts will be developed and tested in order to assess their feasibility.

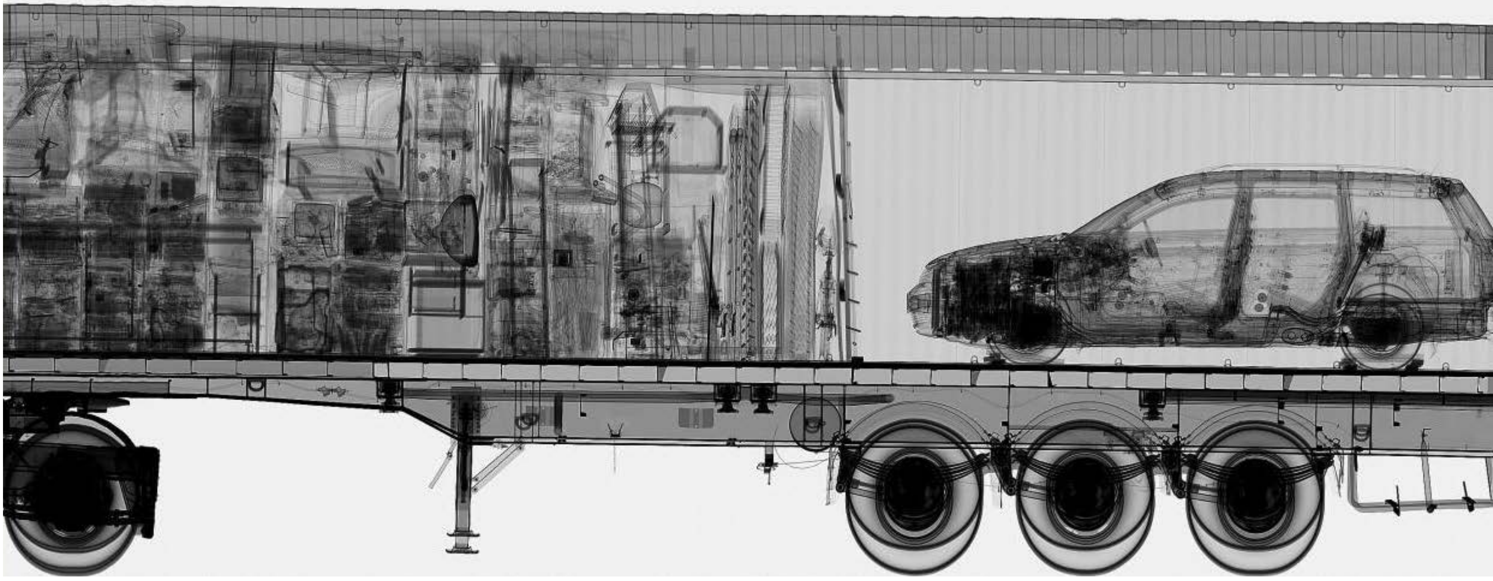
In ABC4EU, special attention will be paid to legal, social and ethical issues and for dissemination and exploitation. ABC4EU consortium considers that all the research carried out in the project has to be compliance to the laws related to border controls in the European Union and respectful to the rights of the European and third country citizens, from the social and ethical point of view.

Expected results

- The need for harmonization in the design and operational features of an ABC System across the E.U. Border Crossing Points (BCPs) is the main goal of the project. The harmonisation and standardisation proposals to be produced by ABC4EU will include requirements and guidelines for all affected parties in the border policy division.
- Contribute towards extending the usage of fingerprint verification, not only as a complement to facial biometrics, but as a fundamental part of border control.
- Development of concepts for the expansion of ABC systems for Third-Country Nationals (RTP, EES and Integration with other Back-Office systems).
- Definition of the concept for the inclusion of BCPs into an Integrated Border Management System (both national and EU level).

PARTNERS	COUNTRY
Indra Sistemas, S.A. (INDRA)	Spain
PricewaterhouseCoopers Auditores, S.L. (PWC)	Spain
Vision-Box, Soluções de Visão por Computador, S.A. (VISIONBOX)	Portugal
Laurea-ammattikorkeakoulu Oy. (LAUREA)	Finland
Eticas Research and Consulting, S.L. (ETICAS)	Spain
Centre for Irish and European Security, Ltd. (CIES)	Ireland
Dermalog Identification Systems, GMBH. (DERMALOG)	Germany
Cognitec Systems GmbH. (COGNITEC)	Germany
Universidad Rey Juan Carlos. (URJC)	Spain
Università degli Studi di Milano. (UMIL)	Italy
SAFE lD Solutions GmbH. (SAFE ID)	Germany
Ministerio del Interior – Spanish National Police. (MIR-DGP)	Spain
Ministério da Administração Interna - Serviço de Estrangeiros e Fronteiras. (SEF)	Portugal
Politsei- ja Piirivalveamet. (EPBGB)	Estonia
Ministerul Afacerilor Interne. (GDCIT)	Romania

ACXIS / Automated Comparison of X-ray Images for cargo Scanning



Information

Grant Agreement N°
312998
Total Cost
€4,771,721
EU Contribution
€3,394,004
Starting Date
01/09/2013
Duration
42 months

Coordinator

EIDGENOESSISCHE MATERIALPRUEFUNGS- UND FORSCHUNGSANSTALT (EMPA)
Center for X-ray Analytics
Ueberlandstrasse 129
CH-8600 Duebendorf
Contact
FLISCH ALEXANDER
Tel: +41 58 765 45 67
Mobile : +41 79 109 26 81
Fax: +41 58 765 11 22
E-mail:
alexander.flisch@empa.ch
Website: www.empa.ch

Project objectives

The main objectives of the project ACXIS are to develop a manufacturer independent reference data base for X-ray images of illegal and legitimate cargo, procedures and algorithms to uniform X-ray images of different cargo scanners and measurement parameters, and an automated identification of potentially illegal cargo.

Historic images of real detections and images of illegal cargo mock-ups as well as images of legitimate cargo will be integrated into the reference data base. This database will automatically analyse the image and will independently inspect uncritical cargo. The new system will be analysed in collaboration with end-users, scientists, and security experts in order to define different threats in cargo screening scenarios.

Current training consists in the identification of a small set of critical cargo elements superimposed on historic images of the inspection system. A draw-back of this system is the adaption of the inspection officer to the small set of training images that are usually limited due to factors like confidentiality of the image data. The set of training images is significantly enhanced if artificial cargo image can be generated with arbitrary positioning of objects in the image data base.

The highly innovative system will be implemented using a simulator to be used in the field by end users in order to ensure optimal results.

Description of the work

The ACXIS project work programme consists of six work packages. The first work package comprises the financial, technical and organisational management of the project. In the second work package, cargo mock-ups will be built and scanned with different X-ray systems. The X-ray images will be integrated in the manufacturer independent reference data base.

Work package three is the development of a data base system to store images of historic detections as well as mock-up images of illegal and legitimate cargo (recorded in work package two) in the standard representation of cargo images to be developed in work package four. In the same work package, methods to streamline the images from different X-ray scanner manufacturers, to reduce background from the containment and to correct artefacts from scattering and imperfect detection systems will be developed to guarantee comparability of the images.

Work package five will develop new concepts for the inspection and automated detection of illegal cargo based on the newly developed data base of reference images. In work package six, the results of all other work packages will be compiled into a working demonstrator that can be employed for on-site presentation of the newly enabled detection capabilities. State-of-the-art computer-based training will be further developed in order to achieve the maximum possible detection by the new cargo inspection system. In work package six, the system will be validated and both exploitation and dissemination activities will be coordinated.

Expected results

ACXIS is expected to:

- A system consisting of three components: a way to transform X-ray images into a standard cargo image, a database filled with images of legal and illegal cargo, and software to determine illegal cargo.
- A database with image analysis that will utilise cargo X-rays for inspection officer training.
- Optimisation of detection system for the maximum benefit of Customs officers and independency on scanner's manufacturer based on end user collaboration and testing.

Implementation of detection software as an add-on to existing scanners independent of scanner's manufacturer.

As both data base and detection procedures are developed based on the reference data type, the resulting procedures can be applied Europe-wide as soon as all manufacturers will provide the corresponding interface.

In the ACXIS project, the tutor system of CASRA for luggage screening shall be expanded for the application on high-energy cargo inspection systems combining the data base, the frame work to generate artificial images and the tutor software system.

PARTNERS	COUNTRY
Eidgenössische Materialprüfungs- und Forschungsanstalt (EMPA)	Switzerland
APSS Software & Services AG (CASRA)	Switzerland
Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	France
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (EZRT)	Germany
Smiths Heimann S.A.S. (SH)	France
Eidgenössische Zollverwaltung (FCA)	Switzerland
Ministere van Financien Directoraat Generaal Belastingdienst (DTCA)	The Netherlands

CONSORTIS / Concealed Object Stand-Off Real-Time Imaging for SecuritySecurity

Information

Grant Agreement N°
312745
Total Cost
€5,132,839
EU Contribution
€3,953,449
Starting Date
01/01/2014
Duration
38 months

Coordinator

TEKNOLOGIAN TUTKIMUSKESKUS VTT (VTT)
Intelligent Sensor Systems
Tietotie 3
P.O. Box 1000
FI-02044 VTT, Espoo,
Finland
Contact
M. Sipilä
Tel: +358 20 722 7007
Fax: +358 20 722 7001
E-mail:
consortiscoordinator@vtt.fi
Website: www.consortis.eu

Project objectives

The project will develop a demonstrator for detection of stand-off real-time concealed objects to support high throughput security screening for European mass-transit markets and infrastructure security.

Description of the work

The technological approach will build on and extend current millimetre-wave imaging technology. The system will undergo an end-user demonstration at a European transport hub.

The ethical issues surrounding the use of stand-off body scanners will be evaluated to ensure that the technology is properly deployed.

The consortium includes end-users as project partners who will ensure maximum relevance and impact to the user community.

The consortium will also address the exploitation of the technology developed in the project, especially the commercialisation and manufacture of the technology through the small and medium sized enterprises involved in the project.

Expected results

A main concrete output of the project will be a live demonstration of the working system at an airport. This demonstration is intended to give end users the opportunity to see the system in operation in a realistic environment.

The results will also include their experience and comments about the system's performance and limitations. From the general public's point of view, the main result will be a better traveller experience with less intrusion into privacy, less encroachment, shorter waiting times and fewer restrictions – all with ethical considerations fully taken into account.

PARTNERS	COUNTRY
Teknologian tutkimuskeskus VTT (VTT)	Finland
Asqella Oy (AQA)	Finland
The University Court of the University of St Andrews (USTAN)	United Kingdom
InnovaSec Ltd (ISEC)	United Kingdom
Totalförsvarets forskningsinstitut (FOI)	Sweden
Eberhard Karls Universität Tübingen (EKUT)	Germany
Wasa Millimetre Wave Ab (WMW)	Sweden
Gotmic Ab (GOTMIC)	Sweden
Finavia Oyj (FNA)	Finland
Rapiscan Systems Ltd. (RSN)	United Kingdom
Technische Universiteit Delft (TU Delft)	The Netherlands

DOGGIES / Detection of Olfactory traces by orthoGonal Gas identification technologIES

Information

Grant Agreement N°
285446
Total Cost
€4,940,117.60
EU Contribution
€3,499,966.00
Starting Date
01/06/2012
Duration
36 months

Coordinator

III V LAB GIE (III-V LAB)
Optronics Devices Research Group
1, avenue Augustin Fresnel
F-91767 Palaiseau Cedex,
FRANCE
Contact
Dr. GERARD Bruno
Tel: +33 (0)1 69 41 57 91
Mobile:
+33 (0)6 82 76 47 76
Fax:+33 (0)1 69 41 57 38
E-mail:
bruno.gerard@3-5lab.fr
Website: www.3-5lab.fr

Project objectives

The key objective of DOGGIES is to develop an integrated sensor system for the detection of illegal substances and hidden persons. This would complement trained dogs currently used in border checks and custom points by police units.

The project aims to demonstrate:

1. an operational movable stand-alone sensor for efficient detection of hidden persons, drugs & explosives;
2. the potential adaptation of this solution to the detection of a much wider range of illegal substances.

One of the main operational challenges is to provide reliable detection in real environments, in particular with the presence of “interferents”.

It is expected that the use of specific pre-concentrators on one hand, and the combination of the signal emerging from advanced software on the other hand will improve the detection reliability.

Description of the work

The initial phase of project starts with the definition of the operational system requirements and the end-users requirements.

Local environmental conditions which could affect the capability of the sensor to detect hidden persons and volatile traces from drugs and explosives are also investigated.

Our project studies only living persons and we first identify the protocols used by canine border teams to collect and store odour samples, and the training process followed by the dogs.

The next phase of the project is devoted to the development of independent building blocks for the realization of the DOGGIES sensors:

» Miniaturised Mid Infra-Red Photo Acoustic Spectrometer (MIRPAS) module for the detection of the target analytes.

The main objective of this task is to build miniaturised photo-acoustic spectrometer (PAS) modules for the measurement of human scent.

» Ion mobility spectrometry

Additionally a mobile prototype of a non-radioactive ion mobility spectrometer with gas-chromatographic pre-separation (GC-IMS) for the identification and quantification of gas-phase trace substances relevant for the overall objectives of the project is developed.

» Data acquisition and fusion

In parallel the appropriate computational methods and techniques are developed in order to acquire the data generated from the measuring units in a reliable way, to process them and to extract the required information using advanced mathematical tools.

The final phase is the operational testing and validation of DOGGIES system.

Expected results

DOGGIES is expected to improve security and safety in Europe and worldwide, and reduce traffics and illegal immigration; taking into account the high financial and psychological costs that result from an act of terrorism, the deployment of DOGGIES would substantially benefit to the entire society.

An expected result of DOGGIES is to produce a final demonstrator efficiently assessed in different relevant operating scenarios.

For the accomplishment of this demonstrator, the following main technical objectives must be achieved:

- Identify the operational specifications and the end-users requirements
- Identify the most relevant VOCs related to human, drugs and explosives or their precursors
- Demonstrate a widely tuneable MIR source, based on quantum cascade lasers arrays multiplexed thanks to silicon-based arrayed waveguide gratings
- Demonstrate a miniature MIR photo-acoustic spectrometer (MIRPAS) module
- Demonstrate a portable Gas Chromatography-Ion Mobility Spectrometer (GC-IMS) module using a non-radioactive ionising source
- Demonstrate selective pre-concentration of the selected relevant VOCs
- Integrate finally in a single portable instrument MIRPAS, GC-IMS, pre-concentrator and gas sampling with data acquisition and fusion software.

As a conclusion, after 28 months, the main building blocks required for the development of an operational movable stand-alone sensor detecting efficiently hidden persons, drugs & explosives, are nearly in place. It is expected that this instrument will be able to complement, if not replace, the dogs currently used by the canine units of the police force, in operations in urban or remote areas such as border and custom points.

PARTNERS	COUNTRY
III V Lab GIE (III-V LAB)	France
Center for Security Studies (KEMEA)	Greece
National and Kapodistrian University of Athens (U.o.A.)	Greece
Gasera OY (GASERA)	Finland
Leibniz-Institut für Analytische Wissenschaften – ISAS – e.V. (ISAS)	Germany
G.A.S. Gesellschaft für analytische Sensorsysteme m.b.H. (GAS)	Germany
Consorzio Interuniversitario Nazionale Per La Scienza E Tecnologia Dei Materiali (INSTM)	Italy
Consiglio Nazionale delle Ricerche (CNR-IMM)	Italy
AEA s.r.l. (AEA)	Italy
Institut National De Police Scientifique (INPS)	France
Université de Nice - Sophia Antipolis (UNS)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LETI)	France
Thales Hellas Anonymi Etaireia Paragogis Emporias kai Ypiresion Ilektronikou Exoplismou (THA)	Greece

EFFISEC / Efficient integrated security checkpoints

© Natalia Bratslavsky - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217991
Total Cost
€16,071,193.27
EU Contribution
€10,034,837
Starting Date
01/05/2009
End Date
31/01/2014

Coordinator

MORPHO
Le Ponant de Paris
27 Rue Leblanc
F-75015 Paris Cedex 15
France
Contact
Krassimir Krastev
Tel: +33 (0) 1 58 11 25 43
Fax: +33 (0) 1 58 11 87 01
E-mail: krassimir.krastev@morpho.com
Website: www.effisec.eu

Project objectives

EFFISEC will provide border officers with up-to-date technologies to

» allow systematic in-depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles, though the use of automatic gates and portable identity checking and scanning equipment;

» provide objective criteria for subjecting some travellers/vehicles/luggage to an extensive check in specific lanes.

Description of the work

Based on a detailed analysis of the operational requirements (including ergonomics, security and legal issues) for all types of borders EFFISEC will focus on four technical key issues: documents and identity check, detection of illicit substances, video surveillance and secured communication.

The technology proposed will be demonstrated for pedestrians, and travellers using cars and buses. Standardisation aspects will be considered and results disseminated.

Results

EFFISEC developed, delivered and demonstrated several ways of improving the in-depth controls of travellers in the land and maritime checkpoints in Europe:

» Integrated approach to border security based on the use of several technological solutions have been proposed: identity checks of travellers, explosives and illicit materials detection, vehicle plate, colour and type recognition, secure communication, hidden objects detection.

» New and unique biometrics-based portable identity checks technology for travellers staying in their vehicles have been proposed and demonstrated.

» Automatic border check gate has been proposed for pedestrians. This gate was combined with the development of a unique X-ray based luggage scanning technology.

» Innovative technologies for very low quantity trace detection of illicit materials have been developed and demonstrated in both land and maritime border conditions.

» Stolen vehicles plate, colour and type recognition system has been proposed.

» Innovative X-ray machine for objects hidden in cars has been developed and demonstrated.

» In depth privacy protection studies in relation to the above mentioned technologies were proposed.

» The project proposed ideas about future standardisation work in these areas.

PARTNERS	COUNTRY
Morpho (MPH)	France
THALES SECURITY SOLUTIONS & SERVICES SAS (THA)	France
THALES ELECTRON DEVICES SA (TED)	France
SELEX GALILEO SPA (GA)	Italy
ELSAG DATAMAT S.P.A. (ED)	Italy
SMITHS HEIMANN GMBH (SDH)	Germany
Sociedad Europea de Analisis Diferencial de Movilidad SL (SEA)	Spain
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Totalförsvarets Forskningsinstitut (FOI)	Sweden
THE UNIVERSITY OF READING (UoR)	United Kingdom
Ministerul Internelor si Reformei Administrative (RBP)	Romania
Microwave Characterization Center SAS (MC2)	France
ADMINISTRAÇÃO DO PORTO DE LISBOA SA (APL)	Portugal
THALES PORTUGAL SA (THP)	Portugal
SECALLIANCE SECURITES INFORMATIQUES SARL (SEC)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
MULTIX SA (MULTIX)	France

FASTPASS / A harmonized, modular reference system for all European automatic border crossing points

© Thinkstock

Information

Grant Agreement N°
312583
Total Cost
€15,485,790.40
EU Contribution
€11,287,715.05
Starting Date
01/01/2013
Duration
48 months

Coordinator

AIT Austrian Institute of Technology GmbH – (AIT)
Safety & Security Department
Donau-City-Straße 1
1220 Wien - Austria
Contact
Markus Clabian
Tel: +43 50550 4294
Mobile: +43 50550 4294
Fax: +43 50550 4150
E-mail:
markus.clabian@ait.ac.at
www.ait.ac.at

Project objectives

FastPass will establish and demonstrate a harmonised, modular approach for Automated Border Control (ABC) for different border control points (land-, sea- and air-) across Europe. The project specific objectives are:

» a harmonised ABC solution that is able to integrate an entry/exit system (EES) and a registered traveller programme (RTP),

» a harmonised ABC usability, based on travellers' feedback, which also helps border guards to focus on potential risks,

» an ABC solution supporting an innovative border crossing concept with interfaces to existing security and infrastructure processes demonstrated at air-, land- and sea borders,

» a European solution and a new European ABC suppliers network.

Description of the work

FastPass brings together key players from the entire ABC value chain - system and component producers, research institutions, government authorities and end-users. The development of a harmonized ABC gate will be accomplished with continuous end-user involvement. The entire innovation process, from components development to the final design of the user interface, will be continuously evaluated by the two end user groups, travellers and border guards. Border control is a major challenge for security and mobility within the EU. Travellers request a minimum delay and a speedy border crossing, while border guards must fulfil their obligation to secure the EU's borders against illegal immigration and other threats. Fastpass will serve both demands at the same time: to keep security at the highest level while also increasing the speed and the comfort for all legitimate travellers at all border control points.

The FastPass ABC process will be designed to address both requirements with equal emphasis. One aspect of aiding a speedy border crossing by legitimate travellers is a harmonised user interface. This will allow frequent travellers from Europe and third country states to pass through an ABC with minimum delay, using the full potential of ID documents. Improved traveller identification technologies, such as new biometric modules, will increase the security of the ABC process and minimise spoofing.

A demonstration and evaluation at all types of borders (air, land and sea) will be implemented in at least three different member states. Compliance with European societal values and citizens' rights is central to the acceptance of the developed technologies, and will accompany the development and end-user interaction throughout the project.

Expected results

FastPass will design a modern border control process, taking full account of privacy, social, ethical and legal issues. This will result in smooth and fast border crossing for legitimate travellers, while ensuring a high level of security. The FastPass solution will provide travellers a seamless, fast border transit harmonized for different (land-, sea- and air-) border control points across Europe and will enable border guards to maintain strict and absolute control which is both unobtrusive and convenient to use.

FastPass will be based on innovative modules that can be standardized across Europe using the experiences of several test installations. The technical design and standards will be open for (European) manufacturers to promote an open standard. The FastPass design will provide border control authorities with a standard, proven design with module options to reduce design, specification and procurement time. This will also provide manufacturers and integrators with a standard design which is simpler, faster and cheaper to build – and easier for customers to understand when comparing designs from different suppliers.

PARTNERS	COUNTRY
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Teknologian tutkimuskeskus VTT (VTT)	Finland
Bundesministerium für Inneres (BMI)	Austria
Österreichische Staatsdruckerei GmbH (OeSD)	Austria
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung E.V (FhG)	Germany
Katholieke Univeristeit Leuvent (KU Leuven)	Belgium
Rajavartiolaitos (RAJA)	Finland
secunet Security Networks AG (secunet)	Germany
Mirasys Ltd (Mirasys)	Finland
Regula Baltija SIA (Regula)	Latvia
The University of Reading (UREADSSE)	United Kingdom
International Centre for Migration Policy Development (ICMPD)	Austria
Tampereen Yliopisto (UTA)	Finland
Gunnebo Entrance Control Ltd (Gunnebo)	United Kingdom
Giesecke & Devrient GmbH (G&D)	Germany
Modi Modular Digits GmbH (Modi)	Germany
Magnetic Autocontrol GmbH (Magnetic)	Germany
JRC -Joint Research Center - European Commission (JRC)	Belgium
ITTI Sp.zo.o.(ITTI)	Poland
Deltabit Oy (deltabit)	Finland
The Chancellor, masters and scholars of the University of Oxford (UOXF)	United Kingdom
Ministerstwo Spraw Wewnetrznych (PBG)	Poland
Finavia Oyj (Finavia)	Finland
Dimotiko Limeniko Tameio Mykonou (PoM)	Greece
Fraport AG Frankfurt Airport Services Worldwide (Fraport)	Germany
Flughafen Wien AG (VIE)	Austria
Intrepid Minds Ltd (IRM)	United Kingdom

FIDELITY / Fast and Trustworthy Identity Delivery and Check with ePassports leveraging Traveller Privacy

© mattjeacock - iStock

Information

Grant Agreement N°
284862
Total Cost
€18,197,463.60
EU Contribution
€12,013,194
Starting Date
01/02/2012
Duration
48 Months

Coordinator

MORPHO
DTS – Technical and Strategic Department
11 Boulevard Gallieni
92130 – Issy les Moulineaux
France
Contact
Sébastien Brangoulo
Tel: +33(0) 1 58 11 87 29
Mobile: +33 (0) 6 31 50 47 51
Fax: + 33 (0) 1 58 11 87 01
E-mail: sebastien.brangoulo@morpho.com
Website: www.morpho.com

Project objectives

Significant efforts have been invested to strengthen border ID checks with biometrics Travel Documents embedding electronic chips (ePassport). However, problems appeared regarding fraud in the ePassport issuing process, including personal data leaks, difficulties in certificate management, and shortcomings in convenience, speed and efficiency of ID checks, including the access to various remote data bases.

FIDELITY is a multi-disciplinary initiative which will analyze shortcomings and vulnerabilities in the whole ePassport life cycle and develop technical solutions and recommendations to overcome them. The project will demonstrate privacy enhanced solutions to secure issuing processes, improved ePassport security and usability, and improved management for lost or stolen passports.

FIDELITY will provide more reliable ID checks, hence hinder criminal movements, and ease implementation of E/E records.

FIDELITY solutions will be designed for backwards compatibility to be deployed progressively in the existing infrastructure. The consortium is composed of market-leading companies, innovative SMEs, renowned academia, ethical-sociological-legal experts, and end-users.

Description of the work

SP1 contains all transversal activities, lasting the entire project duration. It includes consortium management, study of ethical, legal and societal aspects and dissemination actions targeting stakeholders, exploitation planning, external cooperation, and training.

SP2 is the technical start point of FIDELITY. It focuses on security and usability of ePassports and issuance processes. SP2 will analyse shortcomings and specify requirements that will guide the development and assessment of FIDELITY solutions. It will prepare recommendations for stakeholders on how to address shortcomings in ePassports, which will be updated with the outcome of FIDELITY results assessment.

SP3 handles all research and development work related to safer travel document issuance. It will provide as the main outcome recommendations and technical solutions enabling trust in a claimed identity, trust in the identity claimant, and trust in protection of private data.

SP4 focuses on the chain of trust for ePassports. Fast, protected and reliable security schemes for "trustable" verification is the main objective. SP4 includes innovative architectures, different protocol configurations, and the security of ID check devices, which process personal data. SP4 will also provide innovative alternatives to the current certificate chain.

SP5 develops a one-stop check concept. This concept will cover biographic and biometric data, packaged for protected and non traceable queries in multiple databases. ID inspection terminals will be developed based on privacy-by-design principles, to implement this secure and reliable one-stop ID check concept.

SP6 "Travel document of the future" studies advanced ePassport improvements that would be possible only under the condition of revising the current Logical Data Structure (LDS), access protocols to the ePassport, and chip requirements for ePassports and readers.

SP7 "Assessment" covers the development of demonstrators of FIDELITY solutions and their assessment. It will develop a set of demonstrators corresponding to the typical ePassport use cases and will assess, on the one hand, the components developed in SP3-SP5, and on the other hand, the integrated demonstrator.

Expected results

Recommendations for a reliable breeder document, secure ePassport application processes, and fixed and mobile terminals for border control; user-friendly ID check solutions with advanced “on-the-fly” biometric sensors, Privacy-by-Design based solutions, and concepts of next generation travel documents and on how to improve (end-to-end) security and the usability of ePassports. Architecture and protocols for certificates management is also expected.

PARTNERS	COUNTRY
Morpho (MPH)	France
Gjøvik University College (GUC)	Norway
Bundeskriminalamt (BKA)	Germany
Ministère de l’Intérieur, de l’Outre-Mer et des Collectivités Territoriales (FMI)	France
Hochschule Darmstadt (HDA)	Germany
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IGD)	Germany
Alma Mater Studiorum – Università di Bologna (UBO)	Italy
Thales Communications & Security (TCS)	France
Selex Elsag S.p.A. (SEG)	Italy
Central Directorate for Immigration and Border Police (INT)	Italy
Katholieke Universiteit Leuven – COSIC (KUL)	Belgium
Bundesdruckerei GmbH (BDR)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Biometrika (BIO)	Italy
KXEN (KXN)	France
Institute of Baltic Studies (IBS)	Estonia
Centre for Applied Ethics – Linköping University (LiU)	Sweden
ARTTIC (ART)	France

HANDHOLD / HANDHold - HANDHeld OLfactory Detector

© Handhold

Information

Grant Agreement N°
284456
Total Cost
€4,580,959.97
EU Contribution
€3,495,805.59
Starting Date
01/04/2012
Duration
42 Months

Coordinator

THE QUEEN'S UNIVERSITY OF BELFAST (QUB)
Institute of Electronics, Communications and Information Technology (ECIT)
Queen's Road, Queen's Island
BT3 9DT, Belfast,
United Kingdom
Contact
DAVID LINTON
Tel: +44 28 9097 1761
Mobile: +44 7837 716 589
Fax: +44 28 9097 1702
E-mail: d.linton@ee.qub.ac.uk
www.handhold.eu

Project objectives

The main objective is to develop a CBRNE modular sensor platform which is reconfigurable and can be deployed for stand-off detection for periods of up to eight hours, operating on battery power alone. This platform will be capable of stand-alone use, mimicking the operational characteristics of sniffer dogs used to detect drugs and explosives. The project will also develop state of the art sensors for:

- chemical and explosives
- biohazard detection
- RN detection.

While the sensor developments are part of HANDHOLD, the project is more than just a sensor development project. The end user interface and networked supervision of multiple units give Handhold a strategic advantage in tackling border security and enhancing public safety.

Description of the work

Conceptually, the architecture of the HANDHOLD system can be broken down into three distinct layers. Aside from complying with scalability requirements, the system can be used for offline data analysis regarding correlations of spatio-temporal data or to support decision makers- such as enabling a controller to remotely coordinate field operations directly from the headquarters.

The proposal is to build a three-layer architecture:

- Sensors Systems Layer – this layer is focused on the requirements specification for mobile sensors. It includes any commercial sensor that might be acquired in addition to the detailed specifications of the three HANDHOLD family devices that will be developed within the scope of the project.
- Communication Network Layer – this layer will specify all the requirements for the communication server that will operate as a gateway for the data flow between the devices at the Sensors Systems Layer and the HANDHOLD central system installed within the Application Server at the Control Centre system Layer. Field measurements (i.e., sniffed data) are only transmitted to the Application Server if the corresponding sensors are registered within the Communication server. It will support both modes of sensor operation real-time or collect data and send it off-line.
- Control Centre System Layer – this layer contains the HANDHOLD central system (application server) and manages all Client Dashboards which are directly or remotely connected to the application server.

A HANDHOLD platform can be equipped with a single or multiple sensors and can be re-equipped by unplugging one or more sensors and inserting new sensors in their place. In this way the HANDHOLD platform goes beyond the capability of most sniffer dogs as the latter are normally trained to target just one substance. Moreover, the HANDHOLD platform can embrace new sensor technologies as they become available.

The hardware platform and its embedded software will be developed using the latest results from research in hardware and software design methodologies, and will be independent of the target molecules being detected. Individual sensors inserted into the platform will define the operational detection capability of any particular instance of the HANDHOLD platform.

In this way the HANDHOLD device will be capable of being deployed in a range of operational contexts associated with border security and customs controls. This includes but is not limited to:

- Postal inspection and sorting offices

- Maritime container transport
- Baggage inspection at airports
- Inspection of vehicles, ships and aircraft

Expected results

To deliver a prototype at month 24 to test the integration of early stage CBRNE sensors and supervisory systems. This prototype will be evaluated in a controlled but realistic environment. By month 42 a prototype will be delivered for field testing by users that incorporates feedback with smaller size, lighter, longer battery life and integrated supervision.

PARTNERS	COUNTRY
The Queen's University of Belfast (QUB)	United Kingdom
CapnaDSP LTD (CAPNA)	United Kingdom
The Office of the Revenue Commissioners (ORC)	Ireland
Scorpion Networks LTD (SBN)	Ireland
Karlsruher Institut fuer Technologie (KIT)	Germany
DEFENDEC OU (DEFD)	Estonia
INOV, INESC INOVACAO, INSTITUTO DE NOVAS TECNOLOGIAS (INOV)	Portugal
UNIVERSITY COLLEGE CORK, NATIONAL UNIVERSITY OF IRELAND, CORK (Tyndall-UCC)	Ireland
NATIONAL UNIVERSITY OF IRELAND, GALWAY (NUIG)	Ireland

INGRESS / Innovative Technology for Fingerprint Live Scanners

Information

Grant Agreement N°
312792
Total Cost
€4,252,658
EU Contribution
€3,233,782
Starting Date
01/11/2013
Duration
36 Months

Coordinator

MORPHO (MPH)
Direction of Products and Innovation - DPI
11 boulevard Gallieni
92130 Issy Les Moulineaux
France
Contact
Stéphane Revelin
Tel: +33 (0) 1 58 11 32 15
Mobile: +33 (0) 6 75 89 51 09
Fax: + 33 (0) 1 58 11 87 01
E-mail: stephane.revelin@morpho.com
Website: www.morpho.com

Project objectives

For over ten years, the use of fingerprints has been a key technology to help address both identification and security issues around the world. Unfortunately, the overall success of fingerprints for identification and verification purposes greatly depends on the quality of the fingerprints initially enrolled and acquired.

INGRESS aims to research, develop and validate innovative technologies to take fingerprint images. It will pave the way to the manufacture of novel fingerprint scanners capable of properly sensing fingerprints of intrinsic very-low quality and/or featuring superficial skin disorders.

The project focuses on capturing a sub-surface fingerprint and delivering a high-quality image through medical imaging techniques, such as ultrasound, and Full Field Optical Coherence Tomography. Printed Organic Electronics technologies (such as OLED) will also be studied in order to create a new generation of high resolution and mobile fingerprint sensors.

Therefore, the new scanners will be immune to voluntary or involuntary finger alteration, enabling equal access to the biometric technology for all citizens.

INGRESS will evaluate the currently developed technologies and propose a technology development roadmap for the purpose of using fingerprints from identity documents in border control and law enforcement applications.

Description of the work

INGRESS is developing innovative technologies for fingerprint live scanners that support the examination of additional biometrics associated with the finger in order to address the issue of sub par fingerprint images obtained from fingers with superficial skin disorders.

The OCT and ultrasound technologies will make it possible to take fingerprint information under the skin. The patterns that will be revealed thanks to these new techniques will come from the dermis “matrix”. This sub-layer is responsible for the formation of the outer layer. Some biometric elements lying in this deeper layer will then become visible and will enrich traditional fingerprint images, allowing for the creation of a high-quality image. The project also focuses on high definition fingerprint imaging by improving upon some promising new technologies, such as Organic Light Emitting Diodes (OLEDs) and Organic Photo Diodes (OPDs).

Having gathered stakeholders’ requirements, the project will develop several mock-ups (OCT, ultrasound and OLED) at different levels of maturity, in a privacy-by-design approach, which will be evaluated through technology readiness levels. A technological roadmap and a cost study allowing for these mock-ups to reach the product stage will also be defined.

The evaluation will be done via different steps: a laboratory test will verify their performance, and cross compatibility with legacy data and traditional sensors, their ergonomics and the feasibility of a large scale test; then a test on the field with a large set of users will be implemented to validate the relevance of such technologies and prove their feasibility in the context of border control and law enforcement.

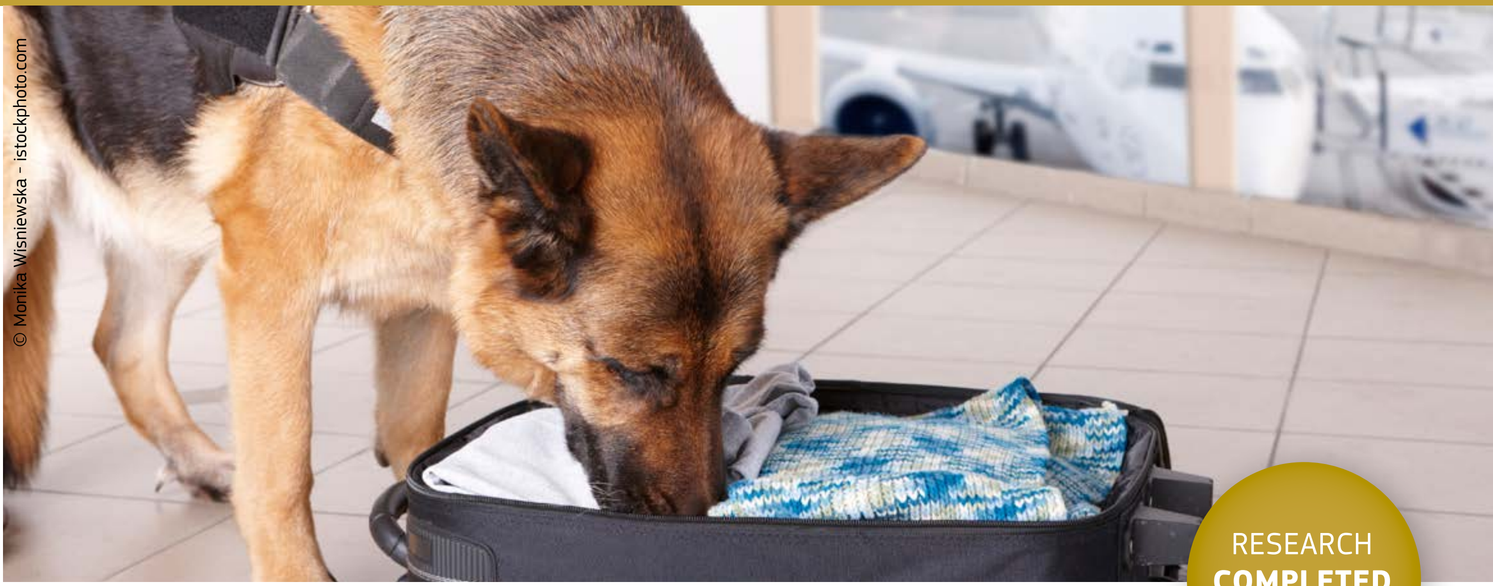
Expected results

INGRESS’ innovative technologies will look and acquire additional biometrics linked to the finger that will complement existing techniques. The solutions proposed in the project offer major improvements to biometrics acquisition. They mainly address the issue of superficial skin disorders by developing hardware and software solutions, while also supporting anti-spoofing detection. The developed technology will greatly enhance image quality and preserve privacy.

The current very low quality fingerprint images of damaged fingers will be overcome by the use of sub-surfacing techniques, which will be the main asset for image quality improvement. This complementarity will deliver high-quality fingerprint images that are still compliant with programs and applications currently using digital fingerprints as a mean of authentication or identification (e.g. EU-Passport, EURODAC, VIS, Entry/Exit, Registered Traveller Program or other European and national applications).

PARTNERS	COUNTRY
Morpho (MPH)	France
Przedsiebiorstwo Badawczo-Produkcyjne Optel Sp Zoo (OPT)	Poland
Alma Mater Studiorum-Università di Bologna (UBO)	Italy
Centre National de la Recherche Scientifique (CNRS)	France
Université de Lausanne (UNIL)	Switzerland
Hogskolen I Gjovik (GUC)	Norway
CSEM Centre Suisse d’Electronique et de Microtechnique SA - Recherche et développement (CSEM)	Switzerland
Turkiye Bilimsel Ve Teknolojik Arastirma Kurumu (TUB)	Turkey
Rijksuniversiteit Groningen (RUG)	The Netherlands
Ministère de l’Intérieur (ST(SI)^2)	France

SNIFFER / A bio-mimicry enabled artificial sniffer



© Monika Wisniewska - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285203
Total Cost
€4,837,982.97
EU Contribution
€3,493,820.72
Starting Date
01/02/2012
End Date
31/05/2015

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Diamond Sensors Laboratory
Centre d'Etudes de Saclay
91191 Gif-sur-Yvette,
France
Contact
Emmanuel Scorsone
Tel: +33 1 6908 6934
Fax: +33 1 6908 7819
E-mail:
emmanuel.scorsone@cea.fr

Project objectives

The SNIFFER project has developed a highly innovative one-stop shop approach to complement sniffer dogs and leverage their capabilities. This approach is based on state-of-the-art technologies centered on a new generation of olfactory biosensors. The SNIFFER devices developed integrate sampling, pre-concentration, and pre-treatment with bio-mimicry, synthetic diamond sensor technology, and multi-parametric training software. This enables the detection of odours arising out of security threats which may occur in a range of border security applications, such as the detection of a broad range of illegal substances carried by people and in suitcases (open or on a luggage belt).

Description of the work

The SNIFFER project was driven by concrete use cases corresponding to major border security applications of artificial sniffing. To make sure it was efficiently managed, the consortium worked with common global milestones, which structured the project in a set of V1 solutions (at midterm) and V2 solutions (at the end of the project).

A first work package defined the usage cases and corresponding metrics, validated them at midterm and at the end of the project and covered the societal and ethical implications of introducing SNIFFER technology in the respective usage contexts. A second work package dealt with the integration and testing of different sub-systems, namely the sampling, pre-concentration, and pre-treatment of target modules developed in a third work package, as well as the multisensory array developed in a fourth work package. Multi-parametric training software was also adapted to cover the broad range of different odours targeted by the project. A whole work package was also dedicated to odorant proteins engineering which is one of the core technologies of the SNIFFER project along with the innovative diamond based transducers. Finally, another work package investigated different aspects of self-diagnostics for artificial sniffers. SNIFFER was a two-step incremental project. A first version of the SNIFFER devices was developed to answer the needs expressed by the users at the beginning of the project (month 1 to 23). A second version was then consolidated taking into account the feedback given by the users on V1 (month 24 to 40).

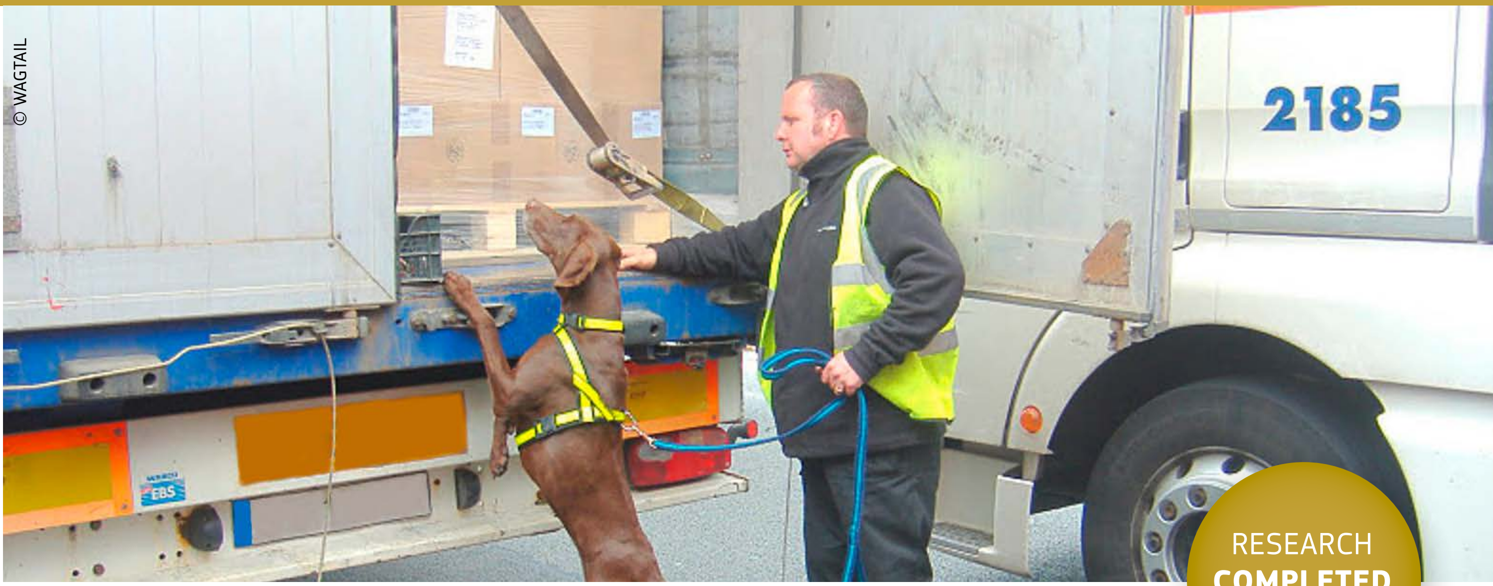
Results

SNIFFER delivered highly sensitive and innovative detection solutions for narcotics and explosives, with special focus on use cases such as body-scanning of people, scanning open luggage, interiors of cars, and closed luggage on running belts. Resulting biosensors have sensitivities in the ppb range for gas phase measurements and for some compounds in solid phase detection to tens of nanograms.

SNIFFER improved a range of technologies and building blocks for future solutions: new sampling, to sniff gas molecules and also particles using electrostatic precipitation (ESP). Improved gas-phase micro-preconcentration, based on porous silicon micro-channels. Ligand Binding Proteins, tailored to bind specific families of narcotics / explosives molecules. New synthetic diamond sensors, immobilising the proteins. Multi-parametric training methods, applied to arrays of LBP-enriched diamond sensors output data, to match macro-patterns against a database, built by exposing the sensor array to large sample sets. Prototypes were assessed in close to real life conditions at Athens Airport. The EU border security community has been confirmed the market potential of future SNIFFER products.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST/LCD)	France
The University of Manchester (UNIMAN)	United Kingdom
Ministère de l'Intérieur - Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure (ST(SI)²)	France
Association pour la Recherche et le Développement des Méthodes et Processus industriels (ARMINES)	France
EADS Deutschland GmbH – Innovation Works (EADS)	Germany
Ecole Polytechnique Fédérale de Lausanne (EPFL)	Switzerland
Centre for Science, Society and Citizenship (CSSC)	Italy
The University of Padua (UNIPD)	Italy
Chambre de Commerce et d'Industrie de Paris (ESIEE)	France
GTP Technology (GTP)	France
TraceTech Security (TTS)	Israel
3D General Aviation Applications SA (3DSA)	Greece
Israel National Police (INP)	Israel
ARTTIC Belgium (ART)	France

SNIFFLES / Artificial sniffer using ion trap technology



© WAGTAIL

RESEARCH **COMPLETED**

Information

Grant Agreement N°
285045
Total Cost
€5,226,007.41
EU Contribution
€3,493,625
Starting Date
01/01/2012
End Date
31/07/2015

Coordinator

TWI LTD
Commercial Group
Granta Park
Great Abington. CB21 6AL.
Cambridge.
United Kingdom.
Contact
Debbie McConnell
Tel: +44 (0)1223 899000
Fax: +44 (0)1223 890952
E-mail:
debbie.mcconnell@twi.co.uk
Website: www.twi.co.uk

Project objectives

The goal of the SNIFFLES project was to develop a Linear Ion Trap Mass Spectroscopy (LIT MS) based device that has a mass range larger than other comparable MS techniques. Additionally, methods for miniaturisation and modularisation were applied to allow reduced vacuum demand and upgradeability. Miniaturisation was made possible through improved designs based on results from modelling, implementation of novel manufacturing techniques and improvements in the MS drive electronics and vacuum system.

The objectives of the SNIFFLES system were to be able to detect weapons, drugs and hidden persons at border crossings; identifying in parallel the elemental, molecular or biological composition all at a high speed of detection.

To ensure the suitability for real world applications the system had a stand-off capability whilst being a complementary technique to that of sniffer dogs.

Description of the work

The areas of work that were undertaken within the project were carried out in 3 phases:

» Phase 1 concentrated on project road mapping that provided a holistic overview of the gas sensor device development, within the context of creating a robust and reliable artificial sniffer. This specified the device performance and enabled all of the individual technical sub-system activities to be undertaken. After this initial output, it continued to run, focussing on forming a structured approach to define the operational procedures of the final device;

» Phase 2 was the technical development of each of the sub-systems that were implemented into the artificial sniffer. Ion trap development ensured a device with high sensitivity whilst using novel manufacturing techniques to create a device with a small footprint and small cost.

The electronic control unit development ensured that the ion trap functions to its highest specification and the measurements taken are accurate and reliable.

The vacuum sub system was technologically advanced to enable the high performance of the system whilst ensuring that the whole system could be contained within the smallest footprint possible.

The operating conditions of the linear ion trap was adjusted to confirm that each stage of the mass spectrometer was operating at its highest performance with the best sensitivity and resolution. The sample inlet operation was designed, enabling the correct operation of the device whilst sampling the multiple substances required.

The end stage of phase 2 was the system integration to ensure that each sub system was working in synchronicity with its partners;

» Phase 3 was where the device underwent its testing and validation program so that the SNIFFLES device was optimised for border control points. The testing integrated a number of development stages including feedback from live field testing trials.

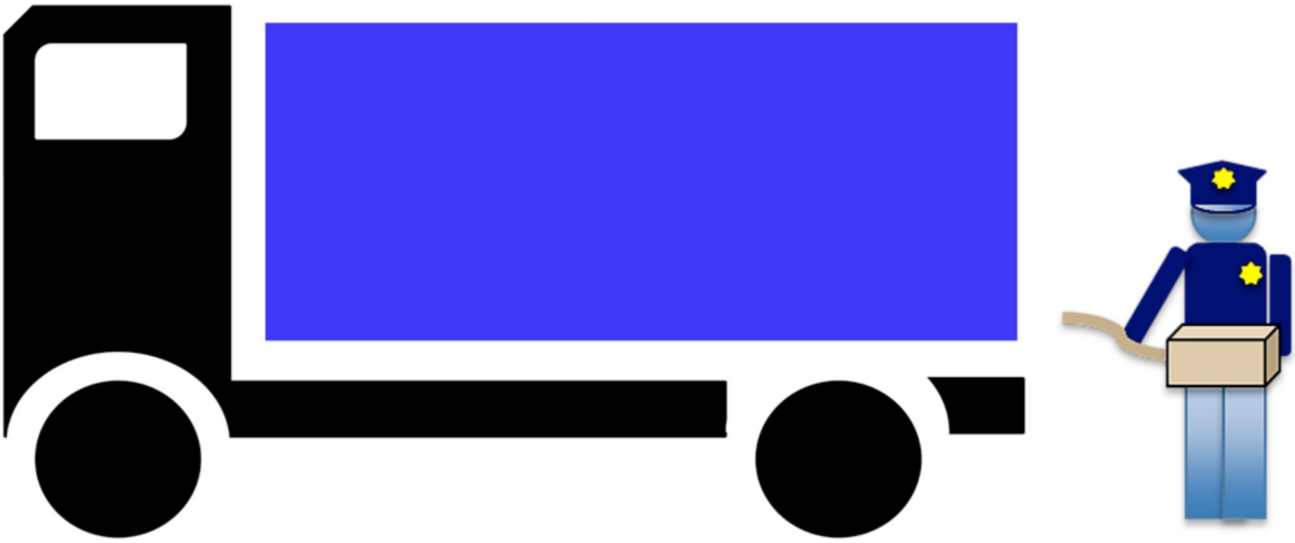
Results

SNIFFLES produced several technical achievements and outcomes. A linear ion trap (LIT) mass analyder was designed, manufactured, and validated in a laboratory environment for the identification of hidden people, drug stimulants (Methyl benzoate, Acetic acid) and explosive stimulants (2-nitrotoluene, Cyclohexanone). The analyser's electrodes and housing were manufactured by 3-D printing to reduce its weight (85%) and cost (70%) and a novel voltage control method (ramped pulse method) was developed to improve LIT resolution (from 4 Da mass peak width to 1 Da with a 500Da mass range). This allowed for a simplified design and lower cost ECU.

The LIT, ECU and battery were integrated into a mobile carry case (400x300x170mm–16Kg) together with a vacuum system containing a high performance-to-size ratio Non Evaporable Getter pump which proved more robust, operated at low power (5W), and was free of vibration compared to turbo molecular pumps. Software development supported LIT design work through simulation and overall system operation, including control of the instrument via a Wi-Fi enabled tablet. Two patent applications were submitted on a glow discharge ion source and non-evaporable getter alloys suitable for hydrogen and carbon monoxide sorption. There has also been the development of a handheld DAPCI ion source for atmospheric sampling into portable and other MS systems. As part of the exploitation plan, a continuation project (ChemSniff) funded under the H2020 SME instrument began in October 2015. This project will focus on reducing system weight and volume, improving reliability and taking the device to TRL7; therefore closer to commercialisation.

PARTNERS	COUNTRY
TWI Ltd (TWI)	United Kingdom
The University of Liverpool (UOL)	United Kingdom
Université Aix-Marseille 1 Provence (UdP)	France
DSM R&D Solutions BV (DSM)	The Netherlands
Q Technologies Ltd (Qtec)	United Kingdom
SAES Getters S.p.A (SAES)	Italy
Envisiontec GMBH (ENV)	Germany
Xaarjet AB (XAAR)	Sweden
Wagtail UK Ltd (WAG)	United Kingdom

SNOOPY / Sniffer for concealed people discovery



Information

Grant Agreement N°
313110
Total Cost
€2,605,284.96
EU Contribution
€1,835,891.00
Starting Date
01/01/2014
Duration
36 months

Coordinator

UNIVERSITÀ DEGLI STUDI DI BRESCIA (UNIBS)
Dipartimento Ingegneria
dell'Informazione
Via Branze, 38
25133 - Brescia - Italy
Contact
Giorgio Sberveglieri
Tel: +390303715771
Fax: +390302091271
E-mail:
giorgio.sberveglieri@unibs.it
Website: www.unibs.it

Project objectives

The SNOOPY project aims to:

» develop an artificial instrument (the SNOOPY sniffer) that identifies the presence of hidden people through the identification of gaseous compounds peculiar of the presence of human beings, arising from, for example, sweat odour;

» defining a metric to calibrate and assess the SNOOPY sniffer performances;

» develop a protocol to integrate the use of already used tools, such as trained dogs and/or ion mobility spectromity (IMS).

In this regard the SNOOPY sniffer will improve the capability of border authorities with respect to illicit traffic of people.

Description of the work

The SNOOPY consortium will address the project objetcives through:

» Development of a pre-concentration unit;

» Development of gas sensors based on different sening and transduction mechanisms;

» development of a pattern recognition software aimed to identify the presence of hidden people in containers based on the sensor array response;

» Creation of a compact prototype based on above technologies;

» Benchmarking of the SNOOPY sniffer with already adopted approaches, namely IMS and trained dogs.

Expected results

The main expected result from the SNOOPY project is a snifter prototype with the following features:

- portable, thanks to the use of low-weight, small size and low-power consumption technologies;
- suited to work in a 24/7 way;
- able to recognize – once trained and calibrated – the sniffed atmospheres on its own, providing the information directly to the user through a display or a set of LEDs, without the need of data transmission and elaboration to remote stations;
- Equipped with a small pipe to collect odours in proximity of small apertures, which are present, for example, at lorry/container doors, even if locked, and from which inner odours can be smelled;
- User-friendly: the SNOOPY sniffer will provide a three-fold output: hidden person present - no hidden person – doubt (in case of doubt the vehicle/cargo will be subject to a more accurate analysis)

PARTNERS	COUNTRY
Università degli Studi di Brescia (UNIBS)	Italy
Consiglio Nazionale delle Ricerche (CNR)	Italy
Università degli Studi di Roma Tor Vergata (UTOV)	Italy
EADS Deutschland GMBH (EADS)	Germany
C-TECH Innovation Limited (CTECH)	United Kingdom
Center for Security Studies (KEMEA)	Greece

TERASCREEN / Multi-frequency multi-mode Terahertz screening for border checks

© Aleksei Potov's

Information

Grant Agreement N°
312496
Total Cost
€4,782,686.32
EU Contribution
€3,489,932
Starting Date
01/05/2013
Duration
42 Months

Coordinator

ALFA IMAGING S.A. (ALFA IMAGING)
C/Rumanía 8 Nave 24
28802 – Alcalá de Henares
Spain
Contact
Naomi Alexander
Tel: +34 91 515 94 16
Mobile: +34 691 221799
Fax: +34 918 827892
E-mail: nalexander@alfaimaging.com
Website: www.fp7-terascreen.eu

Project objectives

The overall objective of the project is to develop and demonstrate in a live border control environment a safe, privacy respecting, high throughput security screening system which automatically detects and classifies potential threat objects concealed on a person.

This will advance state of the art, providing an innovative security screening solution for border and security checks that is effective in terms of both security and operation.

The TeraSCREEN Prototype System will integrate a passive and active subsystem, including the sensor data fusion, image processing and the Automatic Object Detection and Classification, and the Privacy Enhancing algorithms complying with EC Regulation No 1147/2011, respecting fundamental rights and observing the principles recognised by the Charter of Fundamental Rights of the European Union;

Description of the work

Two real-time stand-off imaging subsystems will be developed: a multi-frequency (360GHz, 220GHz and 94GH) Passive subsystem and a 360GHz Active subsystem

Innovative (advancing state of the art) components necessary for the subsystems will be developed, although using commercial-off-the-shelf (COTS) components when available and sharing the components that are common to both subsystems.

Some of these components developed in TeraSCREEN can be exploited in other systems. The performance of the developed components will be summarised after testing in a datasheet-like summary, which will enable exploitation and dissemination of the results. Component packaging, interconnection and transitions will be investigated as part of the component development.

The resulting passive and active subsystems will be integrated. The sensor data fusion and image processing will be developed, along with the user interface. This software will be incorporated into the TeraSCREEN Prototype System, which will then be tested and characterised.

The tests of the integrated system will be carried out at ICTS's VeriSys test facilities where explosive materials can be made available and ICTS's operational knowledge will be used to input into staff training procedures for the Pilot Test. The System will be demonstrated in a Pilot Test at a live control point and passengers will be screened on an opt-in basis.

The ethical requirements and implications for the operation of the TeraSCREEN Prototype System at border checkpoints will be managed throughout the project. The (possibly negative) ethical impact will be compared to the perceived and real benefit created by the TeraSCREEN System.

Expected results

The main project result will be an innovative prototype security screening system. This system will operate at multiple mm-wave and THz frequencies and in both passive and active mode in order to automatically detect and classify objects concealed under clothing. It will screen subjects non-intrusively and in real-time. The concealed object detection and classification will be presented automatically to the operator on a generic computerised silhouette.

The innovative prototype security screening system developed will therefore provide a safe, non-intrusive, privacy respecting, high throughput and high security level solution. The automatic threat detection feature also reduces the level of attention required from the operator, which implies a reduction in the personnel necessary for continuous operation.

This Prototype System will be demonstrated at a live operational control point and its performance there will be evaluated. The results of this evaluation will be another very important project result, proving that this solution can produce consistent and secure results in operational settings, in addition to increasing throughput and respecting privacy.

The components that will be developed to achieve this main project result are also worth including as project results in their own right. Several components will be developed in this project beyond current state of the art.

PARTNERS	COUNTRY
Alfa Imaging S.A. (Alfa Imaging)	Spain
Universidad Pública de Navarra (UPNA)	Spain
Anteral S.L. (Anteral)	Spain
Science and Technology Facilities Council (STFC-RAL)	United Kingdom
Teratech Components Ltd. (Teratech)	United Kingdom
Acreo Swedish ICT AB (Acreo)	Sweden
OMMIC SAS (Ommic)	France
Università degli Studi di Roma “Tor Vergata”	Italy
Goethe-Universität Frankfurt am Main	Germany
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (FHR, FKIE)	Germany
ICTS UK Ltd (ICTS UK)	United Kingdom
Albert-Ludwigs-Universität Freiburg (Uni Freiburg)	Germany

OPARUS / Open Architecture for UAV-based Surveillance System

© Netfalls - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242491
Total Cost
€1,405,309.68
EU Contribution
€1,188,312.75
Starting Date
01/09/2010
End Date
31/05/2012

Coordinator

SAGEM DÉFENSE SÉCURITÉ
27 rue Leblanc,
75015 Paris
France
Contact
Mr Fernando Barbero
Olivier REICHERT
Phone: +33 1 40 70 67 26
Mobile: +33 6 30 97 23 37
E-mail:
olivier.reichert@sagem.com

Project objectives

OPARUS aimed to define an open architecture for operating unmanned aerial systems (UAS) for wide-area land, coastal and sea border surveillance in Europe. This took into account emerging legislation for the safe deployment of UAS platforms across Europe's controlled civil airspace – a regulatory and technical concept known as "air insertion".

The project's technical work focused on surveillance sensors, aerial platforms, secure data links, communication networks and generic ground control stations. Directly connected to the needs of end-users such as Frontex and national Border Guard authorities, OPARUS also looked at cost-efficient solutions to promote maximum efficiency for UAS-based border surveillance operations.

Results

The project held three workshops to define operational scenarios with end-users and receive their feedback on the project results. The first Workshop focused on technology reviews, operational concepts and the definition of scenarios. Based on answers from end-users regarding 29 missions and 15 scenarios, OPARUS identified 26 user requirements that applied to three main geographical scenarios: Poland for land borders, South Mediterranean for coastal and Canary Islands for sea surveillance.

The second workshop proposed architectures for the three missions, with the third presenting the project's final architecture solutions and associated regulatory framework.

Ethical aspects were presented during workshops with close attention paid to identifying applicable European legislation, operational recommendations and proposal for a future roadmap.

For each of OPARUS' four key UAS technologies – sensors, platform, data link and ground control station – a list of generic products and their technical characteristics and performances was defined and classified, including purchase cost estimates. For example, regarding sensors it looked at electro-optical and infrared detection as well as several types of radar.

In the end, OPARUS came up with a set of solutions covering both short-term and longer-term border surveillance needs. Its open architecture includes:

» cost effective surveillance for "typical" border scenarios;

» room for non-proprietary solutions regarding equipment and sub-systems;

- room for SMEs from many member countries to enter the market;
- the ability of companies to share different parts of a complex system which distributes development costs and risks on a broad basis – an advantage that would foster the development of industrial co-operation similar to the Airbus model.

The project's approach to UAS border surveillance architecture, if commercialised, would deliver a system of different classes of technological sub-systems, which end-users could select for joint operations, leading to "more performance instead of heavily competing single systems".

OPARUS proposed innovative solutions for UAS flight operations with today's technology that could be approved by authorities for land or maritime European border surveillance missions.

PARTNERS	COUNTRY
Sagem Défense Sécurité (SAGEM)	France
Instytut Techniczny Wojsk Lotniczych (AFIT)	Poland
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Dassault Aviation S.A.	France
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
Construcciones Aeronáuticas S.A. (EADS-CASA)	Spain
Israel Aerospace Industries Ltd. (IAI)	Israel
Instituto Nacional de Técnica Aeroespacial (INTA)	Spain
Ingeniería de Sistemas para la Defensa de España S.A. (ISDEFE)	Spain
Office national d'études et de recherches aérospatiales (ONERA)	France
Selex Galileo (SG)	Italy
Thales Communications & Security S.A. (TCF)	France
Thales Systèmes Aéroportés (Thales Syst Aero)	France
Tony Henley Consulting Limited (THL)	United Kingdom

SUNNY / Smart UNattended airborne sensor Network for detection of vessels used for cross border crime and irregular entrY

Information

Grant Agreement N°
313243
Total Cost
€14,439,544.88
EU Contribution
€9,569,977.68
Starting Date
01/01/2014
Duration
42 months

Coordinator

BMT GROUP LIMITED
Research
Waldegrave road 1
Teddington TW11 8LZ –
United Kingdom
Contact
Mary Vayou
Phone:
+44 (0)20 8943 5544
Fax: +44 (0)20 8943 5347
E-mail:
m.vayou@bmtmail.com
Website: www.bmt.org

Project objectives

The SUNNY project aims to develop system solutions to improve the effectiveness of EU border monitoring compared to legacy systems whilst keeping the affordability and interoperability as key enabling factors.

Description of the work

SUNNY's objectives are the following:

» Novel sensors and on-board processing generation. The focus will be on developing and integrating sensors of low weight, low cost and high resolution, which can operate under variable conditions such as darkness, snow, and rain. In particular, SUNNY will develop sensors that can generate both Visible, Near Infrared (NIR-SWIR) and LWIR images and hyper-spectral data. It also aims to couple sensor processing and preliminary detection results (on-board) with local aerial platform control, leading to innovative active sensing techniques, replacing low level sensor data communication by a higher abstraction level of information communication.

» The exploitation and adaptation of emerging standard wireless technologies and architectures to the SUNNY scenarios towards the EUROSUR's goal of defining European-wide standards. Existing wireless standard technologies, such as IEEE 802.11a/g/n, IEEE 802.11p, DVB-T2, Mobile WiMAX, LTE, and Wi-Fi@700MHz will be considered due to their low cost and features such as radio resource management, provisioning of high bitrates, and mobility management.

» A two-tier intelligent heterogeneous airborne sensor network will be integrated in order to provide both large field and focused surveillance capabilities. In this network, the first-tier sensors, carried by medium altitude, long-endurance aerial platforms are used to patrol large border areas to detect suspicious targets and provide global situation awareness. Fed with the information collected by the first-tier sensors, the second-tier sensors will be deployed to provide more focused surveillance capability by tracking the targets and collecting further evidence for more accurate target recognition and threat evaluation. Novel algorithms will be developed to analyse the data collected by the sensors for robust and accurate target identification and event detection.

Expected Results

It is recognised that the legacy sensors and communications system developed for military applications are not optimised for border monitoring and their interoperability with civil standards is limited. Moreover, it is acknowledged that the diffusion of the information is tailored in service systems to highly skilled personnel and the number of operators to conduct the activity is high. Via the integration of technologies developed across different initiatives, the SUNNY approach will deliver pre-processed information with meaningful decision support tools enabling the reduction of number and required level of expertise of border surveillance personnel. The SUNNY project aims to contribute to the objectives of EUROSUR by improving sensor and data transmission capacities and real time data processing capabilities.

PARTNERS	COUNTRY
BMT Group Ltd	United Kingdom
Metasensing B.V.	The Netherlands
Xenics	Belgium
Queen Mary and Westfield College, University of London	United Kingdom
Tecnalia	Spain
INESC PORTO	Portugal
Technical University of Crete	Greece
Ministério da Defesa Nacional (CINAV)	Portugal
SPECIM, Spectral Imaging Ltd	Finland
ALENIA AERMACCHI SPA	Italy
TTI NORTE, S.L.	Spain
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
MARLO a.s.	Norway
Vitrociset S.p.A.	Italy
NCSR ‘Demokritos’	Greece
CNIT RASS	Italy
SAAB AKTIEBOLAG	Sweden
ALTUS LSA COMMERCIAL AND MANUFACTURING SA	Greece

CONTAIN / CONtainer securiTy Advanced Information Networking

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261679
Total Cost
€15,525,218.11
EU Contribution
€10,044,904.00
Starting Date
01/10/2011
End Date
31/03/2015

Coordinator

TOTALFÖRSVARETS FORSKNINGSINSTITUT (FOI)
Division of Information and Aeronautical Systems
Gullfossvägen 6, Stockholm
164 90 Sweden
Contact
Pontus Svenson
Tel: +46 8 5550 3732
Mobile: +46 734 44 77 32
Fax: +46 8 5550 3700
E-mail: ponsve@foi.se
Website: www.foi.se

Project objectives

CONTAIN defined and demonstrated a European shipping container surveillance system that encompasses regulatory, policy and standardisation recommendations, new business models and advanced container security management capabilities. When fully implemented, it will:

1. Support public and private transport security stakeholders by managing container security threats within logistic chains as part of an integrated approach to managing door-to-door (D2D) transportation networks;

2. Provide a coherent set of cost effective and efficient technology options for container-integrated sensor, communication and security hardware and software technologies to monitor container movements and security and business related parameters in real time;

3. Enable ports and transport networks to use cost effective upgraded container security processes, including the integration of ICT applications with customs agents and national security forces;

4. Provide added value to investments by EU customs organisations regarding the protection of markets and society, while offering favorable conditions for business via better real time risk evaluation and control;

5. Provide information gathering, validation, fusion and situational awareness services for near real time "corridor container traffic maps" and their integration into an EU container traffic map in support of an EU surveillance policy;

6. Enable secure trade lanes between the EU and selected trading partners;

7. Assist national and EU policy makers to frame container security policy based on sound economic and technological arguments;

8. Support development of European standards for container security and supply chain security.

Description of the work

CONTAIN devised solutions for a risk-based approach to container targeting and scanning, and the optimization of container transport and information interoperability and exchange. Improved positioning, eSeal technology and container security device equipment were developed, and technology solutions for locating containers misdeclared as empty. The results were tested during two small-scale demonstrations in Genoa (December 2014) and Valencia (January 2015) and a large-scale one in Bologna (March 2015).

Results

CONTAIN developed a European containers surveillance framework that includes enhanced sensing technology, decision support systems for authorities and other stakeholders, and methods for using security information to improve business procedures. The results enhance information sharing between stakeholders and authorities, and enable more accurate and timely processing of entry summary declarations and customs declarations. CONTAIN's technology offers more accurate situational awareness of the position and status of containers, thus increasing container handling efficiency for logistics operators. An assessment and benchmarking tool allows users to streamline logistics procedures and improve the efficiency of logistics operators.

CONTAIN's solution supports:

» adaptability, in that systems are able to accommodate new technologies, and extend information exchange agreements with regard to differing legal and regulatory constraints and/or international standards for security,

» scalability, i.e., systems are able to grow or shrink dynamically to meet new challenges including variations of container throughput,

» Resilience, in that failure of a single container monitoring system will only affect the surveillance process as a whole in a minor way.

The results should lead to increased visibility of the supply chain via new and improved sensory and positioning devices, and better situational awareness for logistics operators and authorities. The project's comprehensive toolset, interlinked by the CONTAIN software platform, involves both physical devices and risk analysis software. These have the potential to boost container transportation security by integrating container security data in a common information distribution and sharing environment.

PARTNERS	COUNTRY
BMT Group Limited (BMT)	United Kingdom
Conceptivity Sarl (CTY)	Switzerland
Inlecom Systems Ltd (ILS)	United Kingdom
Consorzio IB Innovation (IBI)	Italy
JRC – Joint Research Centre – European Commission	Belgium
Selex ES SPA (SE)	Italy
Thales Research & Technology (UK) Limited (TLUK)	United Kingdom
Telespazio Spa (TPZ)	Italy
Marlo AS(Marlo)	Norway
Novacom Services SA (Novacom)	France
Teknologian Tutkimuskeskus VTT (VTT)	Finland
MJC2 Limited (MJC2)	United Kingdom
eBOS Technologies Ltd (eBOS)	Cyprus
European Organization for Security SCRL (EOS)	Belgium
Fundaction de la Communidad Valenciana Para La Investigacion, Promocion Y Estudios Comerciales de Valenciaport (VAL)	Spain
Agenzia Delle Dogane (AD)	Italy
Thales Italia Spa (TLIT)	Italy
SO.GE.MAR. Societa Generale Magazzine Raccordati Interporto SPA (SOG)	Italy
Totalförsvarets forskningsinstitut (FOI)	Sweden

EWISA / Early Warning for Increased Situational Awareness

Information

Grant Agreement N°
608174
Total Cost
€13,956,301
EU Contribution
€10,893,914
Starting Date
01/09/2014
Duration
46 months

Coordinator

INSPECTORATUL GENERAL AL POLITIEI DE FRONTIERA
Bd. Geniului 42 C, sector 6
Bucuresti
Romania
Contact
Mr. Andrei VOICU
Tel: +40 743 14 91 54
Fax: +40 21 312 11 89
E-mail: ewisa@igpf.ro
Website: www.ewisa.eu

Project objectives

EWISA aims to assess and improve the management of illegal migration flows at the land border, through greater operational situation awareness and reaction capacity of authorities responsible for land border security. It is also aimed to develop a system in which video-analysis techniques could be combined to serve border maintenance as efficiently as possible and at low cost.

The project objective is to increase intelligence in video surveillance via camera-specific processes and a modular implementation of successive analysis layers, which is applied for optimal situational awareness such as chaining, motion, figure, face. In addition, the network consists of cheap sensors, network analysis and system for control room.

Description of the work

The project proposes to:

1. increase the intelligence of the video surveillance system, detect all the irregular movements within the area and select the suspicious ones conduct in-depth observation and identification of the targets;

2. Achieve 100% surveillance of the overall land border area (water, land, air). Set up and run a demonstration;

3. define the desired interoperability environment, including proposed adaptations to existing systems, to accommodate new capabilities, additional sensors (cameras & radars) and communication media between existing system nodes;

4. to promote the usage of EWISA system concept all over the European land borders

Expected results

The present proposal will provide an innovative system for warning on possible threats, enhancement of effectiveness and efficiency of all security relevant systems, equipment, tools and processes for the surveillance in the selected areas:

- » Sensor and/or radar-video stations, for land and air, placed in high risk areas
- » video analysis techniques that are applicable individually in different border security environments and conditions
    - border surveillance
    - border control (land border)
    - in land checkpoint
- » System design of a multilayer video analysis solution in which different modules, which could be purchased at different times.
- » intelligent video analysis, which offers solutions for the control room personnel. The amount of alarms is reduced to a acceptable level
- » the "false alarm" rate is reduced significantly
- » If the main objective is met, the amount of human labor committed to video surveillance is reduced and the control of video surveillance can be centralized to fewer command centers

PARTNERS	COUNTRY
Politia de Frontiera (Border Police)	Romania
Rajavartiolaitos (Border Guard)	Finland
Guardia Civil (Civil Guard)	Spain
KEMEA (Center for Security Studies)	Greece

GLOBE / Global Border Environment

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218207
Total Cost
€999,891
EU Contribution
€999,891
Starting Date
01/07/2008
End Date
30/06/2009

Coordinator

TELVENT INTERACTIVA S.A.
Mr. Manuel Parra
Av. Valgrande, 6
ES-28108 Alcobendas
Spain
Contact
Víctor Alejandro Luaces Bustabad
E-mail:
victor.luaces@telvent.com
Website:
http://globe.ti-projects.com/

Project objectives

The GLOBE project aimed to produce a comprehensive approach to integrated border management in Europe that factors in the internal, border and global aspects of border management. It set out to assess the existing technical, legal, political and societal environment of Europe's borders, and to suggest information management and integration steps to be taken to enhance border security.

GLOBE was a 'phase one' research project, whose feasibility results will inform a subsequent 'phase two' large scale demonstration project on border management, to be funded in the near future.

Results

GLOBE conducted a comprehensive analysis of current European border management practices, which were compiled into a road-map for future enhancement of these networks.

GLOBE focused, in particular, on the role of the EU's border management agency, Frontex, and bilateral arrangements with the EU's external partners that help member states form an overview of their border management situation.

Two key areas were identified as ripe for further development and synergy in Europe: risk analysis and decision making. GLOBE recommends that the 27 Member States adopt common definitions and criteria for sharing source data, risk analysis results and decision making indicators and reports. Convergence and standardisation in these practices would enable automation in areas such as data gathering, risk assessment and the generation of indicators and reports. GLOBE produced its road-map with these goals in mind.

In the area of border checks, GLOBE focused on potential automated processes for sharing document authentication between member state agencies and external partners. Concepts for innovative technologies to check traveler identity and documents before their arrival at the physical border in order to facilitate the processing in advance low risk passengers were suggested. Supported by an information architecture, this mixture of pre-border document checks and information sharing between neighbours will close loop-holes and expedite legitimate travel, GLOBE concluded.

In the area of border surveillance, maritime border monitoring was identified as a priority. GLOBE works to achieve improved situational awareness and assessment via a fusion of surveillance information with information gathered by all relevant monitoring, reporting and information systems – including those of external partners. Modular networks were recommended for this.

In concluding its project road-map, GLOBE suggests that interoperability and dedicated information architecture should be the focus of the phase two Demonstration Project.

© Fotolia.com

PARTNERS	COUNTRY
Telvent Interactiva S.A.	Spain
Amper Sistemas S.A.	Spain
GMV Aerospace and Defence, S.A	Spain
Instituto Nacional de Técnica Aeroespacial	Spain
Altran Technologies	France
SETTCE	Slovenia
Econet Polska sp. z.o.o.	Poland
Eurosense Belfotop N.V.	Belgium
Skysoft Portugal, Software e Tecnologias de Informaçao, S.A.	Portugal
CES vision Ltd.	Hungary
PRIO	Norway
Empresa de Serviços e Desenvolvimento de Software, S.A.	Portugal
Cogent Systems GMBH	Austria
CIAOTECH Srl (CIAOTECH)	Italy
Fundación Tecnalia Research & Innovation (TECNALIA)	Spain

TALOS / Transportable autonomous patrol for land border surveillance system

© TALOS

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218081
Total Cost
€19,878,692
EU Contribution
€12,898,332
Starting Date
01/06/2008
End Date
31/05/2012

Coordinator

PRZEMYSŁOWY INSTYTUT AUTOMATYKI I POMIARÓW
Aleje Jerozolimskie 202
PL – 02486 Warsaw
Poland
Contact
Mariusz Andrzejczak
Tel: +48 22 874 01 99
Fax: +48 22 874 01 13
E-mail: mandrzejczak@piap.pl
Website: www.talos-border.eu

Project objectives

TALOS is an innovative, Adaptable Land Border Large Area Surveillance System, based on transportable surveillance integrated with rapidly deployable, mobile, unmanned ground and air vehicles, which will address new challenges of external land borders of the enlarged European Union.

The TALOS project proposes to develop an integrated, adaptable land and large area (including devastated environment) surveillance system that:

» Is capable of Detecting, Locating, Tracking and Tracing:

- individuals;
- vehicles;
- hazardous substance.

» Combines remote and autonomous platforms featuring:

- multi sensor data fusion (including biological and chemical);
- active imaging;
- data Fusion;
- command Control & Communication.

The TALOS project's main objectives are as follows:

» To design the Integrated, Adaptable Land Border Large Area Surveillance System based on Unmanned Ground and Air Vehicles (TALOS system);

» To run research works in the main topics addressed by the TALOS project, i.e.: Unmanned Ground Vehicles, Command and Control, Communication, Virtual prototyping;

» To implement the core components of the designed TALOS system as a proof-of-concept prototype in the Integrated Project (IP);

» To set up and run the TALOS demonstrator (prototype) that will show the main benefits of the proposed approach;

» To promote the usage of the TALOS system concept all over Europe, and to contribute to the ongoing efforts of their standardization in Europe;

» To show the cost-effectiveness of the TALOS mobile/transportable concept as opposed to conventional stationary border surveillance solutions.

The main TALOS innovation covers:

» Scalability – its ability to change system scales easily due to changes in the requirements and local conditions such as border size, topography, density of surveillance elements etc.;

» Autonomous capability based on sets of rules (artificial intelligence) - programmed to the computers of the Unmanned ground vehicles and the Command & Control system;

» Mobility/transportability – the whole system will be Mobile/Transportable, installed in standard containers, and transported on trailers for fast deployment in selected border zones (according to intelligence);

» Tactical learning/adaptation behaviour – during the development process, the system will be adapted to local operational requirements, operators will be interrogated and their needs implemented in a system mission planning module;

- No need for fixed infrastructure or fences – the TALOS system, owing to its mobility and transportability, does not require any fixed infrastructure or fences;
- Enables response to intrusion in minutes – system will respond to intrusion in a matter of minutes, not hours; and
- Usage of "green" energy – in remote locations (where it is impossible to connect to standard power lines) the energy will be drawn from natural sources e.g. by means of solar panels (sunny area), wind towers (windy area), water wheels (near rivers).

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Przemysłowy Instytut Automatyki i Pomiarów	Poland
ASELSAN Elektronik Sanayi ve Ticaret A.S.	Turkey
European Business Innovation & Research Center S.A.	Romania
Hellenic Aerospace Industry S.A.	Greece
Israeli Aerospace Industries	Israel
ITTI Sp. z o.o.	Poland
Office National d'Etudes et de Recherches Aérospatiales	France
Smartdust Solutions Ltd.	Estonia
Société Nationale de Construction Aérospatiale	Belgium
STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.	Turkey
Telekomunikacja Polska SA	Poland
TTI Norte S.L.	Spain
Technical Research Center of Finland	Finland
Politechnika Warszawska	Poland

AMASS / Autonomous Maritime Surveillance System

© Volodymyr Kyrylyuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218290
Total Cost
€5,551,702.06
EU Contribution
€3,580,550
Starting Date
01/03/2008
End Date
31/08/2011

Coordinator

CARL ZEISS OPTRONICS GMBH
Carl-Zeiss-Straße 22
DE – 73447 Oberkochen
Germany
Contact
Thomas Anderson
Tel: +49 73 64 20 2833
Fax: +49 73 64 20 3277
E-mail: t.anderson@optronics.zeiss.com
Website:
www.amass-project.eu

Project objectives

The AMASS project sought to develop a surveillance system for the observation and provision of actionable data for securing critical maritime areas against potential illegal immigration; and to help prevent the trafficking of weapons, drugs and illicit substances.

The project aimed to carry out the key research and technological development required to engineer an unmanned platform capable of remotely monitoring maritime areas a considerable distance from shore.

Results

AMASS produced original research into hardware and software solutions for a range of engineering challenges, including: a flotation platform, optronics, hydrophones, communication circuits, power management, image exploitation and command and control systems.

These innovations were tested on the AMASS Prototype, a sea-worthy buoy developed by the consortia. Sea trials in shallow, deep and far off-shore locations were conducted in both the Baltic Sea and Atlantic. During one trial, a rubber boat was tracked at a distance of 5km. In another, communications signal strength was tested for two weeks.

The range of sensors, on-board processing units, transmission technology and platform stabilisation hydraulics required to operate the buoy led to some novel operational adaptations. AMASS engineers also had to optimise a range of existing products to meet the low power consumption, low weight and long life time criteria required by the project brief. A power control unit for managing consumption was developed to optimise energy usage.

The Prototype is also capable of interaction with a base station for basic command and control (C2) functions. For instance, much of the hardware, such as the hydrophonic sensors, can operate in a low-energy “detection mode”, as well as in an on-request high-energy “classification mode” for in-depth analysis of detected signals. Visualisation tools for a C2 hub were also developed, to allow operators to view on-going developments at sea in real-time.

Whilst only one Prototype was actually tested, AMASS has produced a point-to-point radio operating system that can incorporate as many as 65 buoy units with one operating base station.

This highlights the potential to deploy AMASS platforms in an inter-locking network, for 24/7 wide spectrum surveillance of critical maritime areas.

PARTNERS	**COUNTRY**
Carl Zeiss Optronics GmbH	Germany
Crabbe Consulting Ltd	United Kingdom
Armed Forces Malta	Malta
Instituto Canario de Ciencias Marinas	Spain
Fugro Oceanor	Norway
OBR Centrum Techniki Morskiej	Poland
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
IQ-Wireless	Germany
HSF	Czech Republic
University of Las Palmas de Gran Canaria	Spain

CASSANDRA / Common assessment and analysis of risk in global supply chains

© CASSANDRA

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261795
Total Cost
€14,813,514
EU Contribution
€9,958,749
Starting Date
01/06/2011
End Date
31/08/2014

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK
Mobiliteit & Logistiek
Van Mourik Broekmanweg 6
PO Box 49
2600 AA Delft
The Netherlands
Contact
Heather Griffioen-Young
Tel: +31 888 665 931
Mobile: +31 622 461 065
Fax: +31 346 353 977
E-mail:
heather.griffioen@tno.nl
Website: www.tno.nl

Project objectives

The main objective was to enable and facilitate the combination of existing information sources in supply chains for containers into new and better visibility that allowed the assessment of risks by business and government.

CASSANDRA was combining new tools, hardware, visibility platforms and other technical solutions in such a way that business and government were able to fully adopt a risk based approach to their operational activities, and in particular to combine two strategic customs approaches: the Risk-based approach with the System-based audit approach. As such, it was a more balanced approach than the US driven approach aimed at 100% scanning of incoming containers.

CASSANDRA facilitated the adoption of a risk based approach in designing and managing efficient and secure supply chains by business. In addition, CASSANDRA facilitated a dialogue between business and government to gain acceptance of the risk based approach and risk self-assessment by business for supervision by government agencies. This principle of governments' piggy backing on businesses' own risk assessment was becoming a central theme in a number of long term strategies among supervision agencies, such as customs and police.

Description of the work

The main activities in the project were the development of risk based approaches in supply chains and the facilitation of information integration and sharing in the supply chain, by building interfaces between existing visibility platforms, and organizing a consensus building process among business and government agencies to arrive at a commonly accepted framework for risk assessment in the supply chain. CASSANDRA followed very much a data integration and business intelligence approach to risk assessment. As much as possible, this approach relied on existing data sources, data sharing and system integration. Hardware oriented solutions, such as satellite tracking and extensive container scanning, or building completely new platforms or tools were not part of this project.

The project demonstrated and implement this approach to risk assessment in three so-called living labs. These were set up around major European tradelanes: Asia – North West Europe, North Europe – US and North Africa – Southern Europe.

The nine Work Packages were:

- » *WP 1:* Inception and user requirements, ensuring that all partners were at the same level in terms of state of the art and user requirements for supply chain visibility;
- » *WP 2:* Risk based approach, developing the risk based approach to supply chain management, and defining the first draft of a business government interaction protocol on risk assessment;
- » *WP 3:* Design, development and system integration, containing the IT development activities, which consist of interfaces and dashboard development;
- » *WP 4:* Living Lab demonstrations, containing the activities to show the proof of concept in a real life environment;
- » *WP 5:* Evaluation and deployment;
- » *WP 6:* Policy support, privacy and human issues and networking preparations;
- » *WP 7:* Dissemination, networking and consensus building, facilitating further discussion on the business-government interaction that was the result of sharing integral data on supply chain operations;
- » *WP 8:* Scientific coordination;
- » *WP 9:* Administrative management.

Results

CASSANDRA's aim was to enable the combination of existing supply chain information sources with more visibility to allow more accurate risk assessment by businesses and governments. The project developed the concepts needed to increase visibility, facilitate the adoption of modern tools for integrating risk management and screening, and demonstrate these in living labs thus bridging the gap between visibility solutions and community systems. The CASSANDRA solutions are showcased in a serious game: The Chain Game. CASSANDRA engaged in consensus building by providing the platform to discuss and adopt a common risk-based approach for business and government supervision, as well as joint arrangements on how to deal with specific risks. Finally, we carried out various dissemination activities from publications and conference presentations to holding external symposia and workshops.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Erasmus Universiteit Rotterdam (EUR)	The Netherlands
Technische Universiteit Delft (TUD)	The Netherlands
Institut fuer Seeverkehrswirtschaft und Logistik (ISL)	Germany
Fundacion Zaragoza Logistics Centre (ZLC)	Spain
Cross-border Research Academy (CBRA)	Switzerland
GS1 AISBL (GS1 GO)	Belgium
IBM Nederland BV (IBM)	The Netherlands
GMVIS Skysoft SA (GMV)	Portugal
Intrasoft International SA (INTR)	Luxembourg
Atos Origin SAE (ATOS)	Spain
Zemblaz NV (DESCARTES)	Belgium
Senator fuer Wirtschaft und Haefen Bremen (SWHB)	Germany
Ministerie van Financien Directoraat Generaal Belastingdienst (DCA)	The Netherlands
HM Revenue and Customs (HMRC)	United Kingdom
Korps Landelijke Politie Diensten (KLPD)	The Netherlands
Portic Barcelona S.A. (PORTIC)	Spain
ECT Participations (ECT)	The Netherlands
Dbh Logistics IT AG (DBH)	Germany
Seacon Venlo Expeditie B.V. (SEACON)	The Netherlands
BAP Logistics Ltd (BAP)	United Kingdom
Kuehne + Nagel GmbH (K+N)	Austria
DHL Management (Switzerland) Ltd (DHL)	Switzerland
North-South Consultants Exchange LLC (NSCE)	Egypt
Port Authority of Setubal and Sesimbra (APSS)	Portugal
Portbase BV (PORTBASE)	The Netherlands
Integrated Solutions for Ports JSC (ISFP)	Egypt

CLOSEYE / Collaborative evaLuation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions

© Thinkstock

Information

Grant Agreement N°
313184
Total Cost
€12,230,221.51
EU Contribution
€9,218,256.37
Starting Date
27/03/2013
Duration
38 months

Coordinator

Guardia Civil (GUCI)
Mr. JOSÉ MANUEL
SANTIAGO MARÍN
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
C/ Guzmán el Bueno 110
28003 - Madrid
Spain
Contact
José Manuel Santiago Marín
Tel: +34 915146775
Mobile: +34 915146254
Fax: +34 915146264
E-mail: jmsantiago@guardiacivil.es
Website: www.closeye.eu

Project objectives

The main objectives of the CLOSEYE project are the following:

» To provide the EU with an operational and technical framework that would increase situational awareness and improve the reaction capability of authorities surveying the external borders of the EU by following a decentralized approach;

» To validate new security solutions taking into account any aspect of border security that could threaten human rights or break international law;

» To enable public authorities in charge of border surveillance to innovate faster in the provision of their institutional services, making them more efficient and effective;

» To increase the research capacity and innovation performance of European companies and research institutions, creating new opportunities to take international leadership in new markets;

» To conduct pre-operational validation of common application of surveillance tools at EU level via the competitive testing and assessment of several potential solutions;

» To achieve a competitive testing framework

Description of the work

The proposed implementation roadmap for CLOSEYE consists on the implementation of three consecutive phases which include the set of activities necessary to achieve the goals of the Project:

Phase 1: Definition

The definition phase should be based on the latest relevant requirements for European Border Surveillance. CLOSEYE:

» Identification of the needs and the available solutions that could be tested and validated in cooperation.

» Definition of a validation strategy (including a practical exercise plan), setting scenarios and issues for concrete implementation of activities.

» Establishment of good practice procedures and criteria for evaluation and monitoring (common evaluation criteria and implementation methods).

Phase 2: Execution

This phase will implement the validation strategy as prescribed by the CLOSEYE Consortium in Phase 1 (in particular the Call for Tenders for the implementation of testing). During this phase, the providers of solutions to be tested, are to be selected via the competitive call as defined in Phase 1. These providers will execute the testing in real operational scenarios, with their solutions integrated with other existing systems, and working under the supervision of the CLOSEYE Consortium.

Phase 3: Evaluation

In this phase, which will conclude the overall validation, CLOSEYE Consortium will conduct a thorough assessment of the solution performances and cost-benefit ratio of the alternatives tested in Phase 2, against the set of jointly defined performance criteria. This phase includes a set of recommendations that could be extended to other relevant EU organizations.

Expected results

Pre-operational validation guided by end-users, will allow a tangible assessment of the performance levels offered by innovative technologies in a realistic user-defined operational scenario, where a trade off between efficiency, effectiveness and cost can be aligned with actual needs. Moreover, pre-operational validation will allow, not only the assessment of a stand-alone technology, but also the assessment of the integration of the new capabilities provided into current surveillance infrastructure at all levels in the systems' lifecycle (from technical to logistics, training, maintenance, operation and disengagement).

The close link between end-users and industry, especially in those cases where there is a fuzzy perception of the real needs of the user in daily practice for a particular technology, will extend the benefits of pre-operational validation beyond technical development. The identification of innovative applications, business models and procurement strategies will reverberate in the integration of innovative solutions as fully operational tool. By acting as technologically knowledgeable validator of new R&D, the public demand side can drive innovation.

PARTNERS	COUNTRY
Guardia Civil (GUCI)	Spain
Guardia Nacional Republicana, (GNR)	Portugal
Ingeniería de Sistemas para la Defensa de España (ISDEFE)	Spain
Agenzia Spaziale Italiana (ASI)	Italy
European Union Satellite Center (EUSC)	EU
Marina Militare Italiana (MARINA)	Italy

I2C / Integrated system for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat

© DCNS & I2C Consortium - 2011

opyright DCNS & I2C consortium - 2011

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242340
Total Cost
€15,962,707
EU Contribution
€9,869,621
Starting Date
01/10/2010
End Date
30/09/2014

Coordinator

DCNS SA
Direction Systèmes d'Information et de Surveillance
Rond point des artilleurs de marine
B.P 403
83055 Toulon
France
Contact
Michel Morel
Tel: +33 (0) 498 039 259
Mobile:
+33 (0) 699 812 771
Fax: +33 (0) 498 039 257
E-mail: Michel.Morel@dcnsgroup.com
Website: www.i2c.eu

Project objectives

The I2C new generation of maritime surveillance system must allow:

» Permanent and all weather coverage of border maritime areas;

» Continuous collection and fusion of heterogeneous data provided by various types of sensors deployed on shorelines and on mobile platforms and other information from external sources;

» Supervised automatic detection of abnormal vessel behaviours (in track and performed activity) and generation of justified alarms;

» Understanding of suspicious events and early identification of threats from series of detected spatiotemporal abnormal vessel behaviours (alarms);

» Generation of electronic and formatted interpretation reports on suspicious events to keep decision-making authorities periodically informed.

Description of the work

The tasks to perform in the I2C integration project were:

» To set up an end to end information acquisition and processing system;

» To test the fusion of data from a bench of sensors and other available intelligent information sources in order to perform optimal maritime security awareness.

To do so:

» Two coastal sites were installed with a set of sensors. These shore based platforms provided measurements (AIS messages, radar vessel tracks and optical imageries) to elaborate a maritime situational picture for all vessel types. Platforms at sea were also developed (aircraft & vessel patrols, Zeppelin and USV) to provide local node surveillance;

» Fusion of all sensor data with existing information on vessel characteristics (Lloyds Register, Traffic2000, Ship spotting, etc.), on black listed vessels (Paris and Tokyo MOUs), on meteorological conditions (wave height and surface wind speed, etc.) and on geographical data (bathymetry, fishing and protected areas, etc.), took place to provide an intelligent maritime situational picture;

» Applying rules on verified vessel conditions, to detect abnormal vessel behaviours, then sounding alarms for operators for validation. Examples of rules are:

- Vessels boarding during the night and with low wave height will generate an alarm for a suspect event which can be analysed as trans-boarding of goods such as drugs;

- Vessels stopped in international water for less than thirty minutes and with low surface current speed will generate an alarm for a suspect event which can be analysed as dropping smuggled goods at sea.

» Validated alarms are transferred to experts for understanding and identification of threats. Experts use tool kits to analyse the history of the alarm and its evolution over time with the help of knowledge models on similar past suspicious events already identified.

Results

I2C was an integrated maritime surveillance system which used various sensors and assets for detecting vessels over large zones. Sensors included radar such as conventional Frequency Modulation Continuous Wavelength (for small boat detection) and High Frequency Surface Wave (for long-range detection) radars. I2C also used SAR from airborne platforms and other sensors such as electro-optical cameras and AIS sensors (including space borne).

The sensors were incorporated on land, sea, or air assets. Sea and air assets included an aircraft, airship, and unmanned boat. The sensor data and additional AIS from commercial providers were fused and analysed in order to set up accurate vessel unique tracks to form a shared Common Operational Traffic Picture. This picture was then complemented with other data, such as meteo/oceano, ship data, etc. that were fused to produce a Common Intelligent Traffic Picture.

Another component was a tool set for automated detection which alerted on anomalous vessels behavior and facilitation of interpretation of the threat. I2C has performed many real time demonstrations at sea. In particular, it has tested its sensor network, fusion, detection of anomalous behaviour, and threat identification in different scenarios, drug trafficking, illegal immigration, and detection of small floating objects/boats.

PARTNERS	COUNTRY
DCNS SA (DCNS)	France
ROCKVELL COLLLINS France (ROC)	France
FURUNO FINLAND OY (FUR)	Finland
SES ASTRA TechCom SA (AST)	Luxembourg
KONGSBERG NORTCONTROL IT A/S (KON)	Norway
KONGSBERG SPACETEC A/S (KSPT)	Norway
CLEARPRIORITY SA (CLE)	Belgium
ZLT ZEPPELIN LUFTSCHIFFTECHNIK GMBH ET CO KG (ZLT)	Germany
METEOSIM SL (MET)	Spain
AJECCO OY (AJE)	Finland
AIRSHIPVISON INTERNATIONAL SA (AVI)	France
ECOMER (ECO)	France
INTUILAB (INT)	France
SOFRESUD (SOF)	France
ERIC VAN HOOYDONK ADVOCATEN (HOO)	Belgium
ASSOCIATION POUR LA RECHERCHE ET LE DEVELOPPEMENT DES METHODES ET PROCESSUS INDUSTRIELS - ARMINES (ARM)	France
UNIVERSITE PAUL SABATIER TOULOUSE III (IRI)	France
OFFICE NATIONAL D’ETUDES ET DE RECHERCHES AEROSPATIALES - ONERA (ONE)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
DEUTSCHE ZEPPELIN REDEREI GMBH (DZR)	Germany

OPERAMAR / An interoperable approach to European Union maritime security management

© Bruno Delacotte - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218045
Total Cost
€669,134
EU Contribution
€669,134
Starting Date
01/03/2008
End Date
31/05/2009

Coordinator

THALES UNDERWATER SYSTEMS SAS
Route des Dolines 525
FR – 06903 Sophia Antipolis
France
Contact
Bernard GARNIER
Tel: +33 4 9296 3000
Fax: +33 4 9296 4032
E-mail: Bernard.garnier@fr.thalesgroup.com
Website: www.operamar.eu

Project objectives

OPERAMAR aimed to assess the challenges of boosting the seamless exchange of information and ensuring a sufficient level of interoperability between current maritime security management systems amongst EU Member States.

This study had a specific emphasis on technical constraints and legacy systems, but did not ignore organisational and institutional obstacles to information sharing such as legislation and regulations within particular states.

Results

OPERAMAR undertook 40 field visits and stakeholder surveys, which were used to ascertain the current state of information gathering, integration and dispatch between stakeholders in the maritime surveillance field.

The range of actors surveyed included: sea border and port control, customs, fisheries, marine transport and traffic control, marine pollution control, suppression of criminal activities, military actors and marine search and rescue.

In each instance, stakeholders were examined in terms of overall awareness and information management practices during both routine and emergency response activities.

OPERAMAR concluded from these assessments that, given the large number of legacy systems current in operation (estimated at 20 Europe-wide), the following two-pronged approach is recommended:

» A secure and interoperable ICT environment, dubbed the "Common sEcuRe and selective Information Sharing Toolbox" (CERIS.Tbox), should be used as the basis for a shared information sharing protocol that can accept inputs from a variety of existing systems. CERIS Tbox should prioritise common data standards and secure connections – and it should be based on the principle of information "push", whereby data owners retain control over what data is shared with specific end-users;

» Structured around CERIS Tbox, a medium-to-long term vision of operational concepts and technical solutions should be nurtured. OPERAMAR argues that this will encourage future harmonisation and interoperability when managing maritime surveillance activities and response operations.

Overall, OPERAMAR concluded that getting information-sharing to become routine while also developing a common Concept of Operations ("ConOps") are more of an impediment in this domain than the actual technological obstacles.

Next steps:

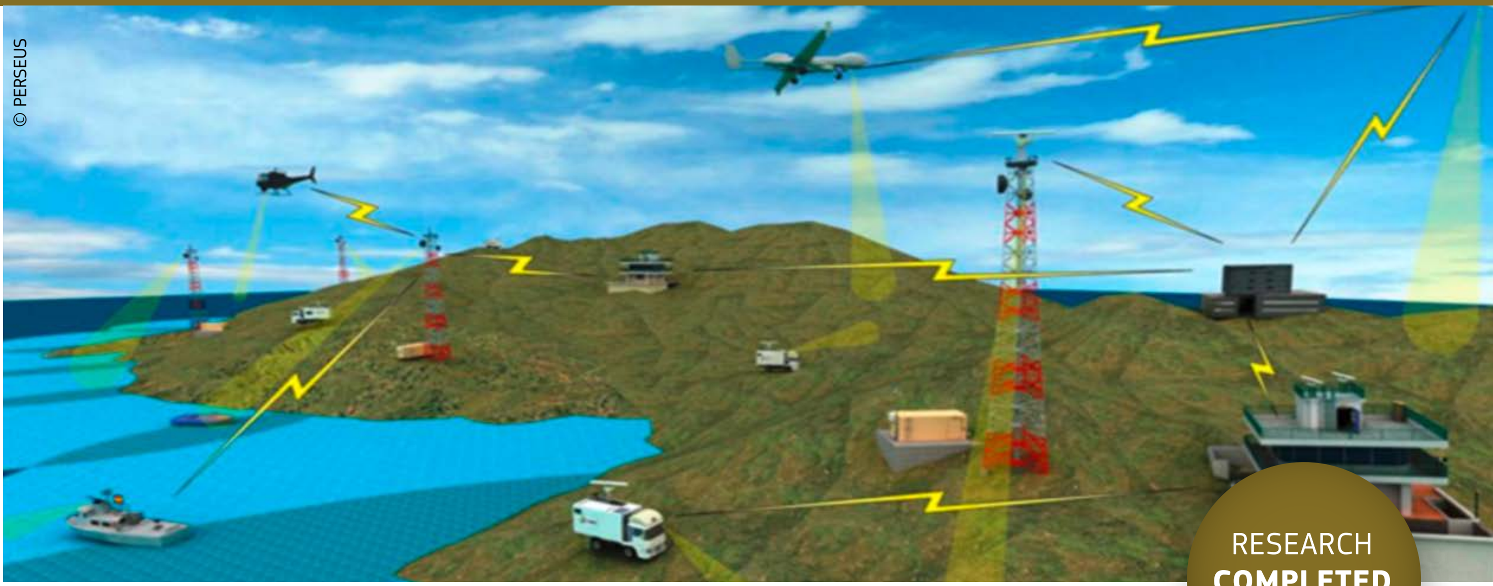
OPERAMAR recommends that an action plan and road-map be developed for two reasons to:

- encourage convergence of member state, stakeholder and EU project efforts related to information sharing, co-ordination and management;
- provide Member States with guidance to enhance their maritime surveillance capabilities, for example in the framework of the EU's External Border Fund.

An over-arching ConOps to create a structured system of integrated maritime management for a European Maritime Domain should also be considered.

PARTNERS	**COUNTRY**
Thales Underwater Systems SAS (THALES)	France
SELEX Sistemi Integrati S.p.A. (SELEX)	Italy
Indra Sistemas S.A. (INDRA)	Spain
Quintec Associates Ltd. (QUINTEC)	United Kingdom
The Alliance of Maritime Regional Interests in Europe (AMRIE)	Belgium
European Commission - Joint Research Centre (JRC)	Belgium
Istituto Affari Internazionali (IAI)	Italy
Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)	Portugal
STM Savunma Teknolojileri Muhendislik ve Ticaret A.S. (STM)	Turkey
Thales Systemes Aeroportes S.A. (TAS)	France

PERSEUS / Protection of European seas and borders through the intelligent use of surveillance


© PERSEUS

RESEARCH COMPLETED

Information

Grant Agreement N°
261748
Total Cost
€43,644,979.60
EU Contribution
€27,847,579
Starting Date
01/01/2011
End Date
30/06/2015

Coordinator

INDRA SISTEMAS, S.A.
Security Systems
Av. de Bruselas, 35
28108 Alcobendas (Madrid)
Spain
Contact
Mr Fernando Barbero
Tel: +34 91 2097937
Mobile: +34 647 624 121
E-mail: fbarbero@indra.es
Website:
http://www.perseus-fp7.eu/

Project objectives

PERSEUS' scope was three-fold, namely to:

» design a system of systems architecture that integratesexisting and upcoming surveillance systems, innovations within PERSEUS and those from other projects to address complex security missions focusing on irregular migration and trafficking

» validate and demonstrate the system of systems Via six surveillance exercises in the Western and Eastern Mediterranean regions

» strongly involve end users for a realistic step by step approach to reach an efficient operational cooperation among the Member States while preserving national prerogatives;

Description of the work

PERSEUS' work had to:

» support a network of national contact centres and Frontex via a communications infrastructure and better surveillance capabilities;

» implement exchanges of information and other procedures to help create a common information sharing environment

» generate a common situational information picture (CSIP), offering tools for surveillance mission planning, decision and interception support, and quasi real-time sharing of information;

» improve detection and identification of non collaborative/suspicious small boats and low flying aircraft;

» enhance automated detection of abnormal vessel behaviours, identification of threats and tracking

Results

Some 40 different technologies were tested and assessed, classified by maturity and proposed for uptake via a procurement model.

The systems, assets and platforms used in real-life exercises included surveillance airplanes and drones of different size and coverage, coastal stations, mobile units, ad hoc communication networks developed for the purpose, and software applications for task orders, collection plans, event dispatching and reports. Also, a new concept of specialised autonomous underwater vehicles was applied to the surveillance of vessels for the first time.

PERSEUS' concept of asset management, including retransmission of information to national contact centres, was implemented. Demonstrations were oriented to the project's two main missions: countering drug smuggling and irregular immigration, but also helping save lives at sea. For this purpose:

a. Outstanding results were achieved by the coast guards during the Western Mediterranean Campaign regarding the detection of small boats in high seas/pre-frontier areas.

b. Similar experience was elicited during execution of the Eastern Campaign, where up to 13 different assets and technologies of maritime surveillance participated in the operational demonstration exercises, together with six different software applications.

PERSEUS created a unique and extensible data model openly available to all stakeholders to interconnect additional systems. This may constitute the base for further developments of a common maritime information sharing environment that could integrate a complex array of information provided by end users and technological partners.

This could pave the way to achieving a common information sharing environment (CISE), as envisioned by the EU. For example, a major result was the commitment and joint involvement of civilian and military bodies in the exercises since PERSEUS enabled cross-sector exchanges of data – significant for progress towards CISE.

Ultimately, PERSEUS delivered a set of nearly 150 conclusions and recommendations, including quantitative and qualitative analysis which should serve as reference for future European initiatives in the field over the coming years

With its set of exercises, PERSEUS helped outline nearly 80 million euros of current and future EU investment in a critical area for Europe's welfare regarding maritime security:

» Several topics for H2020 calls were directly defined from PERSEUS' "technological watch".

» Experience derived from the project is also helping define the contents of future programmes.

» The methodologies, taxonomies and requirements developed in Perseus were applied to the "EUROSUR CONOPS for detecting and tracking small boats" and to the specifications of the "Closeye" project.

PARTNERS	**COUNTRY**
INDRA SISTEMAS S.A. (INDRA)	Spain
EADS DEFENCE AND SECURITY SYSTEMS (EADS-DS)	France
DCNS SA (DCNS)	France
ENGINEERING INGEGNERIA INFORMATICA SPA (ENGINEERING)	Italy
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA (ISDEFE)	Spain
EADS - CONSTRUCCIONES AERONAUTICAS S.A. (EADS-CASA)	Spain
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRD)	Greece
GUARDIA CIVIL ESPAÑOLA (GUARDIA CIVIL)	Spain
INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)	Norway
SAAB AKTIEBOLAG (SAAB)	Sweden
SES ASTRA TECHCOM SA (SES-ASTRA)	Luxembourg
AJECO OY (AJECO)	Finland
INTUILAB (INTUILAB)	France
METEOSIM SL (METEOSIM)	Spain
LUXSPACE SARL (LUXSPACE)	Luxembourg
SOFRESUD (SOFRESUD)	France
INOV, INESC INOVAÇÃO, INSTITUTO DE NOVAS TECNOLOGIAS (INOV)	Portugal
SKYTEK LTD (SKYTEK)	Ireland
LAUREA-AMMATTIKORKEAKOULU OY (LAUREA)	Finland
DFRC AG (DFRC)	Switzerland
BOEING RESEARCH & TECHNOLOGY EUROPE S.L. (BR&TE)	Spain
ECORYS NEDERLAND B.V. (ECORYS)	The Netherlands
CORK INSTITUTE OF TECHNOLOGY (CIT)	Ireland
MINISTERE DE L'INTERIEUR, DE L'OUTREMER ET DES COLLECTIVITES TERRITORIALES DIRECTION DE LA DEFENSE ET DE LA SECURITE CIVILES (MOI FRANCE)	France
FORÇA AÉREA PORTUGUESA (FAP)	Portugal
SATWAYS - PROIONTA KAI YPIRESIES TILEMATIKIS DIKTYAKON KAI TILEPIKINONIAKON EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE (SATWAYS)	Greece
MINISTRY OF NATIONAL DEFENCE, GREECE (HMOD)	Greece
NATO UNDERSEA RESEARCH CENTRE (NURC)	Italy
MINISTRY OF CITIZENS PROTECTION (MCP-HCG)	Greece

SEABILLA / Sea border surveillance

© Colette - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241598
Total Cost
€15,558,125.80
EU Contribution
€9,841,603.55
Starting Date
01/06/2010
End Date
28/02/2014

Coordinator

SELEX SISTEMI INTEGRATI SPA
Via Tiburtina km 12,400,
00131 Roma
Italy
Contact
Salvatore RAMPINO
Tel: +39 06 4150 2407
Mobile: +39 3357389405
Fax: +39 06 41502694
E-mail:
srampino@selex-si.com
Website: www.seabilla.eu

Project objectives

SeaBILLA aims to develop sea border surveillance capabilities to address a number of perceived surveillance challenges in current critical EU regional theatres. The project seeks to:

» reduce the number of illegal immigrants attempting to enter the EU undetected;

» increase internal security by contributing to the prevention of cross-border crime;

» enhance search and rescue capabilities, especially to save more lives of migrants who attempt risky ways to cross the border.

SeaBILLA contributed to these objectives by studying, developing and demonstrating cost-effective solutions for extending, in general, the areas covered by surveillance, with special emphasis on:

» open sea, where surveillance is currently limited to areas with ongoing operations;

» improving the capability to detect small and/or non-reporting vessels typically used by immigrants and illegal traffickers;

» improving the capability to tracks, classify and identify non-reporting vessels.

Description of the work

SeaBILLA is a user-driven project and the user defined scenarios dictated the project work-plan in four project areas:

Project Area 1 (SP1) - Capabilities Roadmap: for each of the above mentioned scenarios, very realistic "vignettes" describing illegal actions have been outlined with the authorities in charge; this baseline of operational requirement has been used to identify the required operational surveillance capabilities, surveillance systems solution, for each scenario, and fill the gaps in legacy systems.

Project Area 2 (SP2) – Surveillance segments improvements: to increase the detection and tracking of small and non-reporting boats focusing airborne, space borne, land and sea based surveillance means available in the near term or new application of existing solutions.

Project area 3 (SP3) - Sensors networking and information fusion: it addresses sensors networking, data fusion and high level processing techniques and solutions which boost the operational capabilities through more effective exchanges of information, correlation tools, data mining engines, abnormal behavior detection etc. from both currently available but not fully exploited information, and from the improved sensor chains.

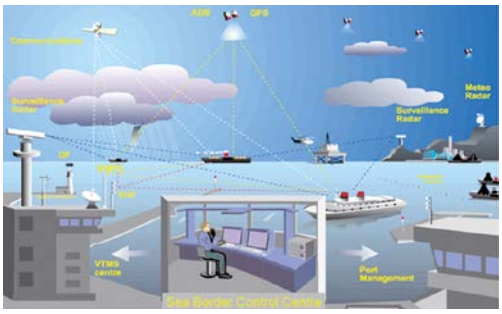
Project Area 4 (SP4) – Trials, demonstrations and validation. SeaBILLA partners, and in particular the associated end-users, will evaluate the effectiveness of the SeaBILLA results of Project Area 2 and 3, through their integration and extensive simulation in laboratories to compare the achieved capabilities in the context of the various operational "vignettes" to measure the improvements respect to the current situation and selected demos on sites for single surveillance sensor or for a sub-set integrated solution.

Results

In agreement with the end user community, Seabilla has focused three main European sea areas (Atlantic, English Channel, Med) where to develop solution to counter specific threats.

The following seven scenarios have been detailed:

1. Atlantic Drug Trafficking
2. Atlantic Illegal Immigration
3. Mediterranean Drug Trafficking
4. Mediterranean Illegal Immigration
5. English Channel Anti-terrorism
6. English Channel Illegal immigration
7. English Channel Drug trafficking



© Seabilla

PARTNERS	COUNTRY
SELEX Sistemi Integrati SPA (SSI)	Italy
Alenia Aeronautica	Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Italy
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Correlation Systems (CorrSys)	Israel
Cassidian S.A.S. (EADS DS)	France
Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)	Portugal
Eurocopter España (ECE) (ECE)	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Holland Institute of Traffic Technology BV (HITT Traffic)	The Netherlands
Indra Espacio S.A. (IE)	Spain
Indra Sistemas S.A. (INDRA)	Spain
European Commission - Joint Research Centre (JRC)	Belgium
Mondeca S.A. (Mondeca)	France
Sagem Défense Sécurité (SAGEM)	France
Space Applications Services N.V./S.A (SpaceApps)	Belgium
Thales Alenia Space Italia S.p.A. (TASI)	Italy
Thales Defence Deutschland GmbH (TMSS)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Telespazio S.p.A. (TPZ)	Italy
Thales Systèmes Aéroportés S.A. (TSA)	France
TTI Norte (TTI)	Spain
University College London (UCL)	United Kingdom
Universidad de Murcia (UMU)	Spain
University of Portsmouth Higher Education Corporation (UoP)	United Kingdom
Thales Alénia Space France (TASF)	France
Thales Communications & Security S.A. (TCF)	France

SUPPORT / Security UPgrade for PORTs

© Herbert Rubens - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242112
Total Cost
€14,629,279.69
EU Contribution
€9,920,607.00
Starting Date
01/07/2010
End Date
30/06/2014

Coordinator

BMT GROUP LTD
Research Directorate
Goodrich House,
1 Waldegrave Road
TW11 8LZ, Teddington, UK
Contact
Jenny Gyngell
Tel: 44 (0)1933 625958
Mobile:
+44 (0)7717 803105
Fax: +44 (0)1933 625958
E-mail:
jgyngell@bmtmail.com
Website:
www.support-project.eu

Project objectives

The project's objective was to support stakeholder groups involved in the security of Europe's major coastal and/or inland ports to build distributed cooperative security systems. SUPPORT optimized the interchange of surveillance and administrative information and threat alerts between port stakeholders, thus promoting a cost effective and multiple use of data in tailored decision support systems.

SUPPORT's solutions provide integrated state-of-the art surveillance/security systems for border control; assist port security operators in decision making; reflect the port's organizational structure and operational modalities; and ensure that differing legal and regulatory constraints and standards for security are met in a cost effective manner.

Description of the work

The work programme analyzed requirements regarding gap-and-threat scenarios, regulations and stakeholder security technology assessment and forecasting. The output led to development of generic models for EU ports security. These were validated by operational experts involved in SUPPORT and were used to help create a 'European standardized approach for port security information exchange and training'.

The generic models were installed in SUPPORT's repository of models and were subsequently used to create service registries for specific ports. These registries contain the information that each port wishes to share on a peer-to-peer basis. Each peer has its own view on the total security information and hence its own tailored decision support system. The generic models also provided the basis for assessing existing systems and simulating appropriate upgrade solutions.

Evaluation took place in terms of improvements to security performance and for cost benefit analysis.

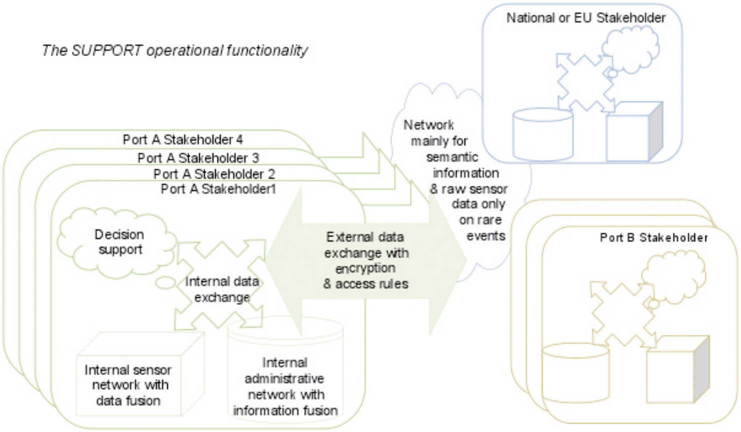
Two full scale demonstrators were created, one representing a state-of-the-art situation and the other focused on typical conditions in European ports.

The demonstrators simulated a full scale installation of the SUPORT platform that included integration with existing systems that helped measure the impact on the security and efficient operation of the ports.

Results

SUPPORT delivered:

- » A “Port Security Management System” as a consolidated and up-to-date self-assessment instrument for maritime security practitioners
- » A “Passive Sea Side Intrusion Detection” capability gear to surface and underwater targets
- » Autonomous underwater vehicles (AUVs) for active threat detection;
- » Training and open-standards based tools to aid security upgrades in EU ports.

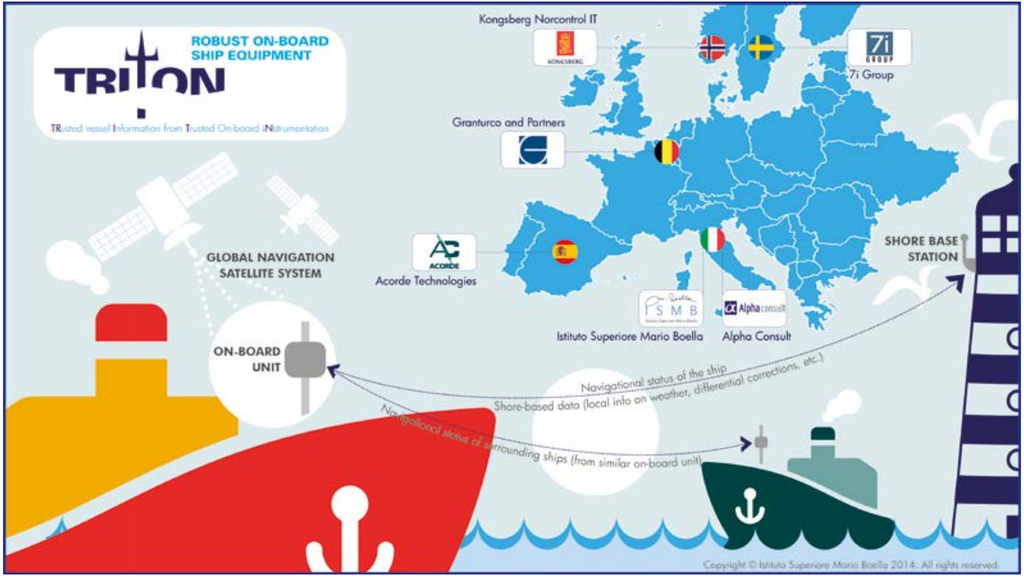

National or EU Stakeholder
Network mainly for semantic information & raw sensor data only on rare events
Port A Stakeholder 4
Port A Stakeholder 3
Port A Stakeholder 2
Port A Stakeholder1
Decision support
Internal data exchange
External data exchange with encryption & access rules
Port B Stakeholder
Internal sensor network with data fusion
Internal administrative network with information fusion

The SUPPORT operational functionality

© Support

PARTNERS	COUNTRY
BMT Group (BMT)	United Kingdom
Swedish Defence Research Agency (FOI)	Sweden
Securitas (Securitas)	Sweden
Technical Research Centre of Finland (VTT)	Finland
MARLO (Marlo)	Norway
INLECOM Systems (ILS)	United Kingdom
MARINTEK (Marintek)	Norway
Nautical Enterprise (NECL)	Ireland
STENA (Stena)	Sweden
eBOS Technologies (eBOS)	Cyprus
University of Innsbruck (UIBK)	Austria
Cargotec Port Security (CA)	Finland
Maritime Administration of Latvia (MAL)	Latvia
INRIA (Inria)	France
MARAC Electronics (ME)	Greece
Port of Piraeus (PPA)	Greece
EUROPHAR -EEIG Port of Valencia - Marseille – Genoa (PV)	EU
ECO SLC (ECO SLC)	The Netherlands

TRITON / Trusted Vessel Information from Trusted On-board Instrumentation


ROBUST ON-BOARD SHIP EQUIPMENT
TRITON
TRusted vessel Information from Trusted On-board iNstrumentation
Kongsberg Norcontrol IT
7i Group
Granturco and Partners
Acorde Technologies
Istituto Superiore Mario Boella
Alpha Consult
GLOBAL NAVIGATION SATELLITE SYSTEM
ON-BOARD UNIT
SHORE BASE STATION
Navigational status of the ship
Shore-based data (local info on weather, differential corrections, etc.)
Navigational status of surrounding ships (from similar on-board unit)
Copyright © Istituto Superiore Mario Boella 2014. All rights reserved.

© Triton_ISMB_A

Information

Grant Agreement N°
312687
Total Cost
€2,151,993.60
EU Contribution
€1,533,099.00
Starting Date
01/12/2013
Duration
24 months

Coordinator

ISTITUTO SUPERIORE MARIO BOELLA (ISMB)
Navigation Technologies Research Area
Via P.C. Boggio 61
10138 – Torino – Italy
Contact
Marco PINI
Tel: +39 011 2276436
Mobile: +39 335 6443351
Fax: +39 011 2276299
E-mail: pini@ismb.it
Website: www.tritonproject.eu

Project objectives

The TRITON project mainly focuses on two objectives. The first is to develop a GPS/Galileo receiver impervious to intentional jamming and spoofing attacks; and the second is to enhance the robustness of the vessel-to-vessel and vessel-to-shore base station communication links . More specifically, the project aims at:

1. Hardening on-board GNSS receivers against spoofing and jamming. Acknowledging the primary role of Global Navigation Satellite System (GNSS) to support ship reporting systems, the project will focus on the GNSS-based positioning system which interfaces with the on-board unit. The goal is to provide a “trusted” GNSS-based source of positioning and timing information, robust against intentional jamming and spoofing attacks, while strenthening a vessel’s ship reporting system.

2. Enhancing ship-to-ship and ship-to-shore communications. TRITON proposes to enforce AIS (automatic identification system) reliability and safety, by adding a new communication channel in the ultra high frequency band. This will be based on layering a secure communication module on top of the standard AIS transceiver. This module will exploit the “white spaces” freed by analog TV, offering a broadband channel that allows several services and enhancements to the current system.

Description of the work

A new awareness has grown across civilian and commercial maritime control stakeholders: that surveillance and safety systems may be under the attack of unintentional or malevolent players, whose aim is to bypass or manipulate control systems to obtain economic gain. The advances of mass-priced technology easily sold over the Internet make this a serious threat that maritime authorities must has cope with.

The TRITON project will research possible solutions to such threats by focusing on enhanced trustworthiness of on-board instrumentation used to report vessel information to the control organisms.

The project starts with the analysis of the state of the art of ship reporting systems, identifying current risks of intentional interference. Such an analysis includes the definition of user requirements based on interviews of stakeholders, end users and experts in the maritime domain. The user requirements and the identified set of risks will be critically analyzed to derive a set of specifications which, in turn, will guide the design and development of the GNSS and communication modules.

The GNSS module will be built on top of a software receiver, able to detect jamming signals and mitigate GNSS spoofing attacks. The countermeasures implemented in the GNSS module are complementary to those provided by GNSS Signal In Space (SIS) authentication. The GNSS module is connected to the robust communication module, which includes a commercial AIS. The frequency diversity provided by the use of white spaces allows for secure mechanisms and a more robust communication in the very high frequency (VHF) segment. The analysis and design of the communication module takes into account the VHF Data Exchange System (VDES) introduced within the e-maritime framework.

In the last phase of the project, the team will have the chance to test and demonstrate the developed technical solutions at the European Commission's Joint Research Centre (JRC).

In addition to its technical work packages, the project foresees a deep analysis from a policy and regulation perspective. This will provide guidelines to future maritime applications as based on the benefits created by TRITON's technologies and methods. TRITON also dedicates a specific task to define a detailed action plan for commercialisation of its research results.

Expected results

At the end of the project, a proof of concept of its proposed technological solutions will be folded into a prototype and appropriate test suites. These will encompass both the robust GNSS receiver and the enhanced communications transceiver. The prototype will be tested at JRC.

Ultimately, the project will boost the understanding of current threats in maritime navigation via its comprehensive analysis of the sector's technological, market-based (cost-benefit) and regulatory aspects.

PARTNERS	COUNTRY
Istituto Superiore Mario Boella (ISMB)	Italy
Kongsberg Norcontrol IT (KNC)	Norway
Acorde Technologies (ACORDE)	Spain
7i Group (7iG)	Sweden
Alpha Consult (ALPHA)	Italy
Granturco and Partners (G&P)	Belgium

WIMAAS / Wide maritime area airborne surveillance

WIMA²S
>> Maritime Traffic Control
>> Anti-Pollution
>> Anti-illegal immigration
>> Search and Rescue
>> Fisheries
>> Smuggling
Voice AIS

© WIMAAS

RESEARCH COMPLETED

Information

Grant Agreement N°
217931
Total Cost
€4,001,123
EU Contribution
€2,737,169
Starting Date
01/12/2008
End Date
30/11/2011

Coordinator

THALES SYSTEMES AEROPORTES S.A
25 Avenue Gustave Eiffel
FR-33608 Pessac
France
Contact
Gilles JURQUET
Fax: +33 (0)5 57 26 71 60
E-mail: gilles.jurquet@fr.thalesgroup.com
Website: www.wimaas.eu

Project objectives

WIMAAS aimed to assess the potential cost reduction, efficiency and enhanced border control benefits for European maritime domain surveillance to be gained via a large-scale integration of unmanned or otherwise remotely piloted airborne vehicles. The project explored the application of such systems for tracking illegal immigration, illegal fishing, smuggling, pollution and terrorist threats.

The final outcome aimed to develop simulation models based on operational scenarios, innovative concepts and technologies for unmanned systems, in-flight experiments, a detailed cost benefit analysis and, finally, a roadmap for the wider use of unmanned aerial vehicles (UAVs), including R&T priorities and future program suggestions.

Results

The primary outcome of the project was the exploration of a future “system of systems” (SoS) architecture incorporating UAVs to produce complete maritime domain awareness.

The first step of the project was to gather and analyze the future needs of potential End-Users in charge of maritime surveillance on European borders. End-user consultations included 10 national and military authorities, plus Frontex. This led to the generation and simulation of scenarios such as drug trafficking between North Africa and Spain, illegal fishing in the Aegean, illegal immigration between Libya and Italy and a theoretical terrorist hijacking in the strait between Cyprus and Turkey.

WIMAAS was considered as a generic system including all airborne platforms (PF) in the maritime 3rd dimension. The notion of system covers the platforms, their sensors, airborne or ground Command and Control system to coordinate PF tasks, to exploit data before transmission to SoS, and the communication system enabling data exchange between platforms with crews, and between PF and SoS.

Further research aimed to develop the multi-sensor concepts required to integrate UAVs into existing maritime domain awareness processes.

On board processing and fusion is analysed for observation payloads to reduce data throughput transmission, to improve levels of automation, to decrease the amount of exchanged data and to reduce data link bandwidth, paving the way for miniaturisation of the airborne mission segment.

The Sensor and data fusion concepts on the ground address the definition of a solution to reach a level of situation awareness, which allows the timely detection and prevention of events threatening maritime security and the environment. The challenge is rather to process and represent them in an intelligent and meaningful way to give sufficient information support to human decision-makers.

Dynamic tasking provides an aid to decide the path of aircraft in the area of interest. The issue is to dynamically plan the path of the airborne platform in order to comply with the mission objective (reach in a specified time an observation position) periodically updated by real time detection or objects of interest generated by its own sensor or by an external sensor. An algorithm has been developed and experimented.

A crew concept was also developed to assess the personnel requirements and workload management needed to operate UAVs from a central base station. An optimal mission length and crew size was aggregated from a series of mission scenarios.

A communication study has defined an innovative architecture for complete data communications between air vehicles and the ground segment, introducing innovative access techniques and interfaces.

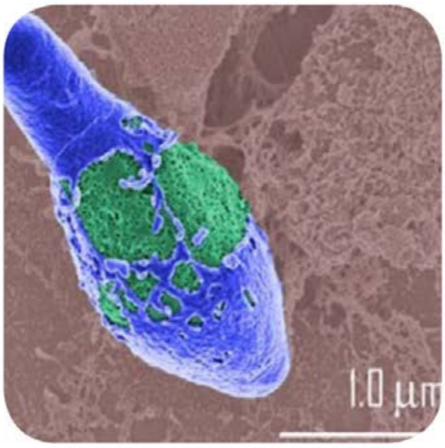
The project concludes that there is no single multipurpose UAV platform capable of covering every altitude and maritime environment. A multi-platform category system-of-systems would be required.

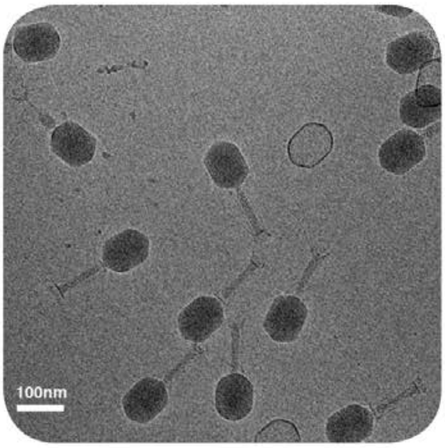
To facilitate further research into this, WIMAAS concluded with a cost estimate based on varying degrees of mission intensity and the use of multiple (up to 10) types of UAV platforms. These cost estimates, excluding training and maintenance expenses, can now form the basis of a policy assessment for implementing a wide maritime area surveillance network based on UAVs.

PARTNERS	**COUNTRY**
Thales Systemes Aeroportes S.A	France
SELEX GALILEO	Italy
Dassault Aviation	France
SENER Ingeneria y Sistemas	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
Air Force Institute of Technology	Poland
EUROSENSE	Belgium
SATCOM1 Aps	Denmark
SETCCE	Slovenia
Aerovisión Vehículos Aéreos S.L	Spain
Thales Communications S.A.	France
Mediterranean Academy of Diplomatic Studies	Malta

ANTIBOTABE / Neutralising antibodies against botulinum toxins A, B and E

© AntiBotABE





RESEARCH **COMPLETED**

Information

Grant Agreement N°
241832
Total Cost
€3,896,416
EU Contribution
€2,966,386
Starting Date
01/09/2010
End Date
28/02/2015

Coordinator

Ministère de la défense (MLD)
Institut de Recherche
Biomédicale des Armées
(IRBA), Département des
Maladies Infectieuses, unité
Interaction Hôte-Pathogène
1 Place du Médecin Général
Inspecteur Valérie André
BP73
91220 Brétigny sur Orge,
France.
Contact
AVRIL Arnaud
Tel: + 33 (0)1 78 65 10 72
Fax: + 33 (0)1 78 65 19 60
E-mail: arnaud.avril@irba.fr
Website: www.antibotabe.eu

Project objectives

Botulinum neurotoxins (BoNTs) are the most toxic substances currently known, and they are possible bioweapons. Naturally-occurring food intoxications, though rare but often severe, are still encountered and intoxication due to the cosmetic use of an unapproved batch of therapeutic BoNT has also been reported. Despite extensive research, no small synthetic specific molecule has been validated for therapeutic use against BoNTs. In Europe, the sole specific treatment relies on an old stockpile consisting in horse polyclonal antibodies, which is poorly tolerated. Recombinant antibodies are the most successful class of therapeutic molecules of biologicals. The goal of AntiBotABE was to develop recombinant antibodies neutralising BoNT A, B and E, which are the subtypes implicated in the majority of natural human-intoxications. Antibodies against the heavy and light chains of BoNT A, B and E were developed to obtain a synergistic effect.

Description of the work

This project started with the immunisation of 6 non-human primates (NHP) with non-toxic recombinant proteins, representing the light or heavy chains of BoNT A, B and E. The lymphocytes of NHPs immunised up to a high titer with these immunogens, were used for the construction of six immune phage-displayed libraries. These libraries were screened to isolate high-affinity antibody fragments (scFvs), which are considered as human-like due to the high identity between non-human primates (NHP) and human antibodies. ScFvs cross-reacting with the subtype A1 and A2, and B1 and B2, were isolated with a specially-designed panning procedure. To test for neutralisation capacities, scFvs or scFv-Fc (an IgG like format) directed against heavy chains were tested in in vitro and ex vivo assays, and the scFvs directed against the heavy chains were tested in vitro. For each library, the most neutralising scFv was selected and super-humanised. The super-humanisation of NHP antibodies has been described as an approach that decreases the potential immunogenicity of therapeutic antibodies. In effect, due to the physiology of the immune system, antibodies undergo affinity maturation processes, that bring mutations in antibody regions involved in tolerance. These mutations cause differences between the human germline encoded segments, part of the immunological self, and those of the immunoglobulins G (IgG). We have shown that "super-humanisation" (also called "germline humanisation") of NHP antibodies is possible, by reversing most of these mutations while respecting the affinity. This process was applied to the 5 neutralising scFvs isolated in the course of the project. In the third part of the project, neutralising, super-humanised scFvs were expressed as full-sized IgGs and tested in a standardised protection model to verify their efficacy against several strains and toxin subtypes of BoNT/A, B and E. At various steps of the project, our results were communicated to the first responders more particularly involved against bio-threats

Results

AntibotABE thus developed successfully a recombinant, protective human-like antibody cocktail against A, B and E botulinum toxins.

Five IgGs were produced targeting the light or heavy chain of Botulinum toxins A, B and E. The IgGs were proven to be protective in non-lethal and lethal in vivo assays in mice. They showed a strong synergistic effect when combining an anti-heavy and an anti-light chain antibody directed against the same BoNT serotype.

Currently, the clinical and regulatory development of the antibodies is planned.

In addition, AntibotABE has allowed to successfully demonstrate the antibody development process which can now be applied to a wide range of therapeutic application.

PARTNERS	COUNTRY
Ministère de la défense (MLD)	France
Technische Universitaet Braunschweig (TUBS)	Germany
Institut Pasteur (Pasteur)	France
Medicines and healthcare products regulatory agency (MHRA)	United Kingdom
Centre National de la Recherche Scientifique (CNRS)	France
LFB Biotechnologies (LFB)	France
Helsingin Yliopisto (UoH)	Finland
Absiskey (Absiskey)	France

BOOSTER / Bio-dosimetric tools for triage to responders

© Tommy Windecker- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242361
Total Cost
€4,583,559.24
EU Contribution
€3,284,291
Starting Date
01/07/2010
End Date
30/06/2013

Coordinator

COMMISSARIAT
A L'ENERGIE ATOMIQUE
ET AUX ENERGIES
ALTERNATIVES
CEA LIST – Digiteo Labs
91 191 Gif-sur-Yvette
FRANCE
Contact
Marie-France ROBBE
Tel: +33 (0) 1 69 08 87 49
Fax: +33 (0) 1 69 08 60 30
E-mail:
marie-france.robbe@cea.fr
Website:
http://www.booster-project.org/

Project objectives

The effective management of an event involving the exposure of numerous people to radioactive material, whether accidental or following a malevolent act, requires a mechanism for the rapid triage of exposed individuals.

BOOSTER aims to develop new bio-dosimetric tools and to integrate them into a toolbox to quickly evaluate the level of potential casualties after a radiological event, and allow for an efficient triage of exposed people.

The project's objectives were: rapid evaluation of radiological incidents by sensors and retrospective dosimetry, development of new fast-acting biodosimetric sensors and adaptation of existing methods and devices, and the integration of all sensors in a portable toolbox usable by first responders, and for the training of first responders.

Description of the work

The BOOSTER System architecture was conceived to fit current procedures for radiological crisis management, based on the definition of different areas. The exclusion and controlled areas are defined from the radioactivity levels measured. The equipment used in the controlled area allows the cartography of the radiological situation: dose-rate-meters (Colibri & GPS-COM) for real time radiological measurements, rugged PDA for live information from first responders, gamma camera (Gampix) for hot spot location, and portable detector (FALCON 5000) for identification of radionuclides.

Results

The BOOSTER project developed a global and unique toolbox for:

» quickly assessing the radiological situation in the field,

» evaluating the radiological dose received by each victim and the toxicity of products used during the attack,

» speeding up the categorization and triage of exposed individuals.

It also allows for potential follow-up material for medical staff in the medium/long term after an event.

PARTNERS	COUNTRY
Commissariat à l’énergie atomique et aux énergies alternatives	France
AREVA CANBERRA	France
Hungarian Atomic Energy Authority	Hungary
Center for Energy Research of the Hungarian Academy of Sciences	Hungary
Karlsruher Institut für Technologie (KIT)	Germany
National University of Ireland, Galway (NUI Galway)	Ireland
Universidad Politécnica de Valencia (UPV)	Spain

CATO / CBRN crisis management: Architecture, Technologies and Operational procedures

© Bruno Vincent - Getty Images

Information

Grant Agreement N°
261693
Total Cost
€14,148,292.23
EU Contribution
€10,278,062
Starting Date
01/01/2012
Duration
36 months

Coordinator

NESS A.T LTD
Ness Technologies and Systems Group (TSG)
Kiryat Atidim
P.O.B. 58180
Tel Aviv 61581, Israel
Contact
Victor Remez PhD.
Tel: +972 3 5483664
Mobile: +972 52 6076516
Fax: +972 3 5483578
E-mail:
Cato-coordinator@eurtd.com
Website: www.cato-project.eu

Project objectives

- **To deliver a comprehensive Toolbox addressing the needs of all stakeholders:** Policy Makers, Incident Managers, Healthcare providers, the Population and Responders.

  CATO addresses the entire disaster life cycle: preparedness, monitoring and detection (alerts and early assessment), response and recovery;

- **To develop a flexible, open, and innovative approach** to cope with the issue of fragmentation between current approaches, systems, and organisational set up.

  The CATO Toolbox should provide the means to build a dedicated customised DSS (Decision Support System) adapted to local and national organisational, political and financial constraints as well as different levels of exposure to CBRN threats;

- **To create an Open DSS-Architecture for the CATO CBRN Toolbox** to be adaptable to the specific context of the CATO-DSS's owner;

- **To Focus on Users and Organisational Learning:**

  CATO is to set up a **CATO Laboratory**, a simulation based environment where Policy Makers can see scenarios in action, evaluate their impact and develop strategies, and CBRN experts can validate and demonstrate new CBRN scenarios etc.

Description of the work

CATO is organised in 8 Sub-Projects (SPs):

- *SP 1* **"Planning, Response & Ethics"** gathers the main effort from the "user partners" and provides requirements and feedback through validation & testing;

- *SP 2* **"CBRN Expertise"** gathers the CBRN scientific experts together, to support the project with advice on hazardous materials, and systematically collect and provide best practice references;

- *SP 3* **"CATO Core and Knowledge Base"** focuses on the central architecture of the CATO system;

- *SP 4* **"Algorithms"** focuses on CBRN algorithms for data and information fusion, threat detection, propagation & evaluation, holistic situation assessment and decision support;

- *SP 5* **"CATO Interfaces"** covers both the user and the system interfaces providing the basic infrastructure for interoperability with existing systems;

- *SP 6* **"Integration"** puts together the CATO Laboratory to validate the CATO approach with users and the CATO Proof of Concept;

- *SP 7* **"Dissemination"** aims to build a dedicated user and expert community, and establish a regular and deep dialogue with this community;

- *SP 8* is dedicated to **Management**.

CATO pursues several strands creating a virtuous learning process:

- Dialogue on CBRN crisis management between stakeholders and experts, leading to a deeper understanding of the issues at stake and influencing the developments. CATO, by design, will be open to collaboration with third parties on a mutual benefit basis. CATO expects progressively to have access to a broad range of results in return for access to the CATO Toolbox;
- Development of sub-systems of the CATO Toolbox;

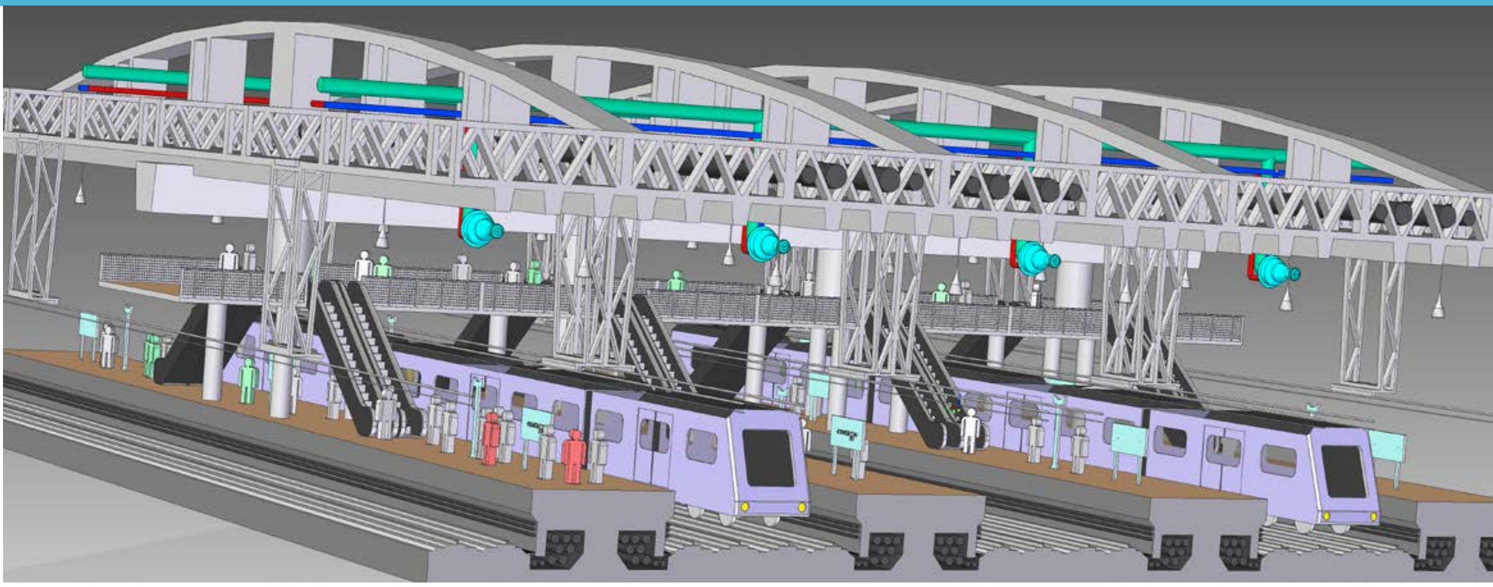
- » Research activities in exploiting written input from the population, correlating multiple data analysis of fuzzy data, and data and information fusion;
- » Implementation of a first prototype DSS which will serve several purposes:
  - Allow for the validation of the CATO approach with different CBRN scenarios;
  - The "field based proof of concept" will allow the CATO project to test the CATO approach for the entire life cycle and especially the debriefing and "feedback" added into the CATO knowledge base;
  - The CATO Laboratory will provide a strong basis for **validation, testing, dissemination** and future **exploitation of results**;
  - A continuous stream of dialogue with the stakeholder community.

Expected results

- » Create a basis for the production of more effective operational CBRN toolboxes, by progressively incorporating results of tests and simulations;
- » Facilitate knowledge collection and sharing around a "simulation based" dialogue;
- » Improve the capability to manage the complexity of CBRN crises by fusing heterogeneous multi-source information into a common picture and offering alternatives for reaction;
- » Enable policy makers and managers to go through accelerated learning, and testing of response strategies for given scenarios and facilitate the exchange of best practices.

PARTNERS	COUNTRY
Ness A.T. Ltd. (Ness TSG)	Israel
VectorCommand Ltd (VCL)	United Kingdom
Police National CBRN Centre (PNCBRNC)	United Kingdom
Prolog Development Center (PDC)	Denmark
Technical University of Denmark (DTU)	Denmark
Danish Emergency Management Agency (DEMA)	Denmark
Studiecentrum voor Kernenergie/Centre d'Etude de l'Energie Nucléaire (SCK-CEN)	Belgium
ARTTIC (ART)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Service de Santé des Armées (SSA)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Centre for European Security Studies (CESS)	Germany
Robert Koch Institute (RKI)	Germany
Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)	Germany
Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH) (HMGU)	Germany
Hospital University of Bonn (UKB)	Germany
University of Jyväskylä (JyU)	Finland
Technical Research Centre of Finland (VTT)	Finland
University of Salzburg (PLUS)	Austria
National Radiation Protection Institute (SURO)	Czech Republic
VÚJE Trnava (VUJE)	Slovakia
Inconnect (INCONNECT)	The Netherlands
Magen David Adom (MDA)	Israel
Center for Science Society and Citizenship (CSSC)	Italy
Peace Research Institute Oslo (PRIO)	Norway

COUNTERFOG / Device for large scale fog decontamination



Information

Grant Agreement N°
312804
Total Cost
€4,417,089.40
EU Contribution
€3,471,992.70
Starting Date
01/11/2013
Duration
48 months

Coordinator

UNIVERSIDAD DE ALCALA (UAH)
Departamento de Teoría de la Señal y Telecomunicaciones
Escuela Politécnica Superior. Campus externo
N-II km 33,600
28805 - Alcalá de Henares
Spain
Contact
JOSÉ LUIS PÉREZ-DÍAZ
Tel: +34 918856746
Fax: +34 616689298
E-mail: Jl.perezd@uah.es
Website: www.counterfog.eu

Project objectives

COUNTERFOG will design, build and test a rapid response system for combating dispersed CBRN agents by using a fog made of a solution that could eventually contain any kind of neutralizing component. It should not only be suitable to be "incorporated" into a fog fire protection system in buildings, but also be able to be used in open air conditions. It is intended to provide a very fast and early response, greatly reducing the number of potential fatalities.

It is intrinsically an environmental-friendly and electric-compatible system. It would have three benefits: First, neutralizing and collapsing the CBRN cloud, second, rapidly decontaminating all the affected people in that area, and finally, rapidly decontaminating any equipment and the facility itself. It will be possible to counteract a CBRN cloud in large, open areas.

A Fog Dynamic Laboratory will be designed, built and used in the project to test the ability such a system has to condense different kinds of smokes, clouds or fogs and its ability to simultaneously neutralize different kinds of CBRN agents and combined incidents. A portable prototype will also be developed for full scale tests.

This project will also determine the best neutralizing agents and will characterize the effects and performance of the system. Eventually, the real applicability, side effects and compatibility with conventional fire protection facilities will also investigated.

Description of the work

Computer aided engineering tools, the most recent manufacturing techniques and new materials are combined to design and build a "COUNTERFOG" generator able to produce an efficient neutralizing/decontaminating fog.

A laboratory for testing the fog dynamics will be designed and built as well. This will be used for experiments to determine the fog dynamics, fog dynamic interaction, condensation and neutralization with fogged decontaminates. It includes testing the harmfulness of the best decontaminants using small laboratory animals.

Other auxiliary technologies will be also developed as a simple sensor for monitoring the progress of the decontamination or new agents particularly useful for this kind of system.

A system prototype will be installed onboard a truck and a second one will be installed in a large building. Finally, full scale tests both in a large building and at open-air sites will be completed.