Project No.
COOP-CT-2006-032585
Project acronym
SAFETALK

Project title

THE DEVELOPMENT OF A CONTINUOUS SWEEP RF HARMONIC SPECTRAL ANALYSIS DETECTOR

Instrument: Co-operative research projects

Thematic priority: Horizontal Research Activities Involving SMEs

PUBLISHABLE FINAL ACTIVITY REPORT

Period covered: from **Month 13** to **Month 27**

Date of preparation: **31/03/2009**

Start date of project: **01 December 2006**

Duration: **27 months**

Project coordinator name: **Anna Jabłonowska**
Project coordinator organisation name: **Innowacja Polska Sp. z o.o.**

Revision: **1**

Section 1 – Project execution

1.1. A summary description of project objectives

Theft of intellectual property and confidential information is a growing threat to a large number of European SMEs, adversely influencing their competitiveness in the global knowledge based economy. There is a need to address this problem by actively preventing the use of electronic devices in knowledge theft. The SafeTalk project delivers a system in the form of a walk-through portal that will reduce the risk of intellectual property being stolen.

€120 billion is lost to Intellectual Property theft in Europe every year alone, with additional uncountable loss in competitiveness and fraud that can be attributed to the intentional use of electronic devices for capture, storage and transmission of confidential information. A significant proportion of this crime is from 750,000 innovative, high-tech European SMEs. The losses incurred by knowledge theft impact on other sectors such as the 120,000 commercial law firms (predominantly SMEs) and 250,000 SME accountants and 200,000 SME insurers.

These eavesdropping devices if not detected have the potential to steal Billions of Euros of 'secret knowledge' from unprotected, knowledge-reliant SMEs. The only current counter-measure is "sweeping", which costs around €4,000 for a "sweep" service, potentially €48,000 yearly for monthly coverage per SME, very few of which can actually afford it. Specifically, the system developed will bring a preventative measure for both large and small knowledge-reliant companies - a new affordable integrated detection and identification system that integrates the key technology elements of developed NLJD technology, into an arch architecture system capable of detecting a threat to IPR capable of detecting the threat of an individual's ability to steal secret knowledge, for which there is no currently available alternative.

The SafeTalk allows for detection of various types of electronic devices that prevents owners of surveillance devices from entering information-sensitive areas and prevents potential sensitive knowledge theft attempts.

The main strategic objective of the SafeTalk proposal was to provide knowledge reliant SMEs across Europe with a new integrated security system capable of addressing primarily the buying drivers of performance and functionality by offering both large and small companies a solution capable of detecting the threat of an individual's ability to steal secret knowledge, for which there is no currently available alternative. By achieving this, we will address the Directives on the Enforcement of Intellectual Property Rights EP-PE_TC1-COD(2003)0024, adopted by European Parliament, understanding the importance of protecting this vital asset. This innovative technology will help increase the competitiveness of the SME Community through the development of export and licensing opportunities outside of Europe.

The scientific objectives of the project involve the extension to current knowledge of:

1. Characterisation mechanisms for definition, possible detection and analysis of device harmonic signatures incorporating multiple non-linear junctions, including required RF field strengths, modulation schemes for a probe signal and exposure time required, and the optimal set of harmonic signature characteristics (amplitudes of harmonic signals, phase shift and group delay) that can be used to constitute harmonic signature of a device discriminating false non linear junctions and providing sufficient information for device classification (OBJECTIVE MET).
2. Issues of RF signal acquisition in relation to multiple space diverse receivers including optimal antenna design, receiver sensitivity, selectiveness of filters, measurement time and complexity required, repeatability and robustness in the face of interference or ability to reject interference (OBJECTIVE MET).
3. Estimation of SAR in the limbs and torso of a person at the nominal operating distance and the spectrum regulatory framework that the devices will have to exist within (OBJECTIVE MET).

4. Harmonic signature analysis using fuzzy logic paradigm for classification purposes and neural network for matching with patterns stored in database library populated for different types of electronic surveillance devices (OBJECTIVE MET).

By meeting the scientific objectives, the project is expected give rise to the following technologies:

- A method for reliable detection and characterisation of harmonic answers from devices incorporating non-linear junctions (OBJECTIVE MET)
- An apparatus for classification and matching harmonic signatures on the basis of harmonic answers from electronic devices (OBJECTIVE MET).

The overall technical objective is to produce a commercially viable system, at a suggested retail price of €7,000, for detection and identification of 85% of available electronic surveillance equipment, passing through a doorway into a protected room, laboratory or workspace. In addition, **specific technological objectives** need to be satisfied to enable the system to:

1. **Permanently detect the presence of any electronic device** passing through an arch of a volume of $4m^3$ through the RF illumination of the concealed device using a deliberately modulated probe signal and subsequent analysis of a conjugated harmonic response generated by the non linear junctions in the device. The envisaged probability of recognition of a semiconductor junction will be 97% (OBJECTIVE MET).
2. **Analyse the RF harmonic responses** and accomplish signal processing for device detection and identification based on an average walking speed of 5 km/h. The technical objective is to develop a **signal conditioning unit** performing demodulation, as well as FFT analysis for discrimination of 2^{nd}, 3^{rd} and higher order harmonics, as well as known clock signals capable of providing within 100ms operational time an information vector necessary for building harmonic signature (OBJECTIVE MET).
3. **Ensure compliance to EMC regulations** and health & safety issues. Specifically, the worst case SAR (Specific Absorption Ratio) must meet the ICNIRP guidelines and comply with the new EU directives on safe limits of RF exposure by developing **microstrip antenna systems**, the **RF transmitter** and **receiver** that will in implemented into the **plastic arch structure**, thus limiting the sensing distance to 1 m (OBJECTIVE MET).
4. **Store up to 100 RF harmonic signatures of known electronic surveillance devices** within a specially designed reconfigurable database interacting with the decision unit to ensure that at least 85% of the various types of electronic eavesdropping devices can be detected. The first 25 of the 100 harmonic signatures will be loaded onto the database within the timeframe of the project and using the prototype arch produced by the project (OBJECTIVE MET).

1.2. Contractors involved in the project

SME PARTNER 2 NATEL

Nature of Business
Navtel Systems (NATEL) are experts in providing advanced signal processing based on their reconfigurable hardware modules around open technology.

Role in the project
Their role in the project was to participate during the design, development and manufacture of the signal conditioning and decision unit, in WP3, especially in tasks 2A and 2B with the implementation of algorithms for classification of captured signal development.

SME PARTNER 3 SFTMND

Nature of Business
SoftwareMind (SFTMND) are an innovative software house operating in the global market, providing highest-quality, proprietary IT products and services for companies from the telco, and financial and banking sectors and medium and large enterprises. The company's offer includes solutions that support the management of sales processes, business relations, and client-related information as well as design and implementation of dedicated

IT solutions, modelling of EAI architectures, management and organisation of software production processes, and quality audits.

Role in the project
SFTMND provided input in all areas related to software development; it in particular worked on harmonic signature database development within WP2. In addition, based on their expertise, the company contributed to the design of the Decision Algorithm within Task 2B and its implementation.

SME PARTNER 4 TTI

Nature of Business
TTI is an SME established in 1996 in Spain and active in the area of RF and antennas technology for telecommunications applications. Nowadays TTI is a company working in the state-of-the-art and forefront technologies of key industrial sectors: space, defence, science and telecom. TTI has expertise in different and related technological fields: antennas, RF & Microwaves and Control & Power Supply Devices.

Role in the project
They participated in the development of the antenna system and user panel (WP3), together with advisory contributions in WP1 and WP2.

SME PARTNER 5 ETRONIC

Nature of Business
EC Electronics (ETRONIC) are active in the electronic projects development. They have experience in piezoelectric technology, especially in dedicated electronics for machine vibration monitoring, diagnostics and tests. ETRONIC undertakes electronic product design, development and manufacture. With leading edge experience gained across a wide range of industries, they are able to provide an integrated and innovative electronics solution for Hi-End products.

Role in the project
ETRONIC supported and guided activities in WP5 and WP6 to ensure the enabling technologies are validated, integrated and installed in the most efficient and robust fashion. ETRONIC is the official system integrator.

SME PARTNER 6 TSE

Nature of Business
TSE is a manufacturing company active on domestic as well as international markets in four product spheres, three of which have a common base - electronics and electric engineering while the fourth is based on mechanical engineering. They offer co-operation on development, design and production of electronic components, assemblies and products.

Role in the project
TSE provided the fabrication service to the hardware for the arch architecture including the assembly of associated cable wiring looms. They provided the communication links between the detection technologies, the process control technology and the central database reporting software.

SME PARTNER 7 INTOR

Nature of Business
Inicjator (INTOR), is a Polish law firm specialised in IPR protection. The key area of their business are services related to patent protection, advice and support in the legal aspects of the commercialization process, and handling of acquisition issues in sales: licenses of protected solutions and know-how licenses, assessment of values of trademarks, house brands, patents, know-how and other nonmaterial assets.

Role in the project
INTOR was very keen to participate and exploit the results of developments that were taking place within our project. The nature of their business requires very high standards of confidentiality which is the key for building trust with customers. During the project, they were specifically involved in providing input to end-user requirements across work packages.

SME PARTNER 8 AUTEN

Nature of Business
AUTEN is a leader in authentication solutions for brand protection and fiscal recovery. Formed in 2003 from the merger of Isotag, Biocode and Calyx, the company has twenty years' worth of experience in providing overt and covert authentication solutions to many pharmaceutical producers. Within the range of solutions that it provides, AUTEN authenticates dosage forms as well as their packaging. The company has a wide expertise in the field of overt colour shift inks, which enable an initial visual inspection for authenticity, as well as covert and deep forensic security features, which are only detectable via specialist readers. AUTEN is specialized in making multi-layer solutions such as: colour shifting ink, pen revealable marker, laser authentication, spectral finger print A and B, molecular markers.

Role in the project
As a high-tech blue chip SME, they played an important role in the provision of specialist end-user knowledge required for the application of the new technology for protection of confidential knowledge. Specifically, they provided input to end-user requirements and co-ordinated training activities for validation within WP5.

In order to bring the SAFETALK from the drawing board to the manufacturing stage, the SMEs, which had a lack of sufficient research capability of their own, sourced two RTD providers with a deep understanding of, and the capability to provide a unique technological step change solution to the problem.

Research and Technology Developers (RTDs)

PARTNER 1 InnowacjaPolska

Business Activities

InnowacjaPolska is a leading independent high technology research organisation in Central and Eastern Europe, with a highly respected international client base. They provide research and technology development services for the design and development of customised software for industrial applications and high level electro-mechanical design, development and installation. They have experience in the design and development of sophisticated wireless systems for acquisition of data from remote sensors using different transmission protocols. Their expertise includes also the development of solutions for storage and processing of multidimensional data, network system development and integration. InnowacjaPolska operates within a non-profit distributing corporate structure with an objective to generate and transfer new technology to industry, providing step change improvement in competitive advantage for industry as a whole. They have experience in the design and development of customised electronics, DSP expertise, RF system development, signal conditioning and integration of systems. INPOL is not an IPR holding or exploiting business.

Why was it selected?

InnowacjaPolska has important skills in electronics engineering and has direct expertise in the areas of development of electronic sensor and special purpose electronics incorporating intelligence. This experience includes deep knowledge of the use of various microwave electronic components and appropriate design methods. InnowacjaPolska has successfully completed a number of relevant projects, such as Vibcon – remote data acquisition for remote monitoring and control, through the application of similar skills that will be required in this project including wireless sensor development. The skills of the key technical staff cover all the aspects related to the research in the field of designing optimal microstrip antenna layout and leads, selecting proper electronic components, designing microwave electronics and circuits, ensuring temperature stability of super high frequency electronics and digital signal processing. The project will enlarge for them the geographic span of their activities developed through the partnerships with the industrial partners as well as science and research

institutions participating in the project. Through involvement in this project, InnowacjaPolska has benefited by extending their expertise in the design of microwave devices and signal processing.

Partner 9 CRIC

Business Activities
CRIC is a multidisciplinary research centre based in Spain, which aims to help small and medium enterprises to be more competitive through technology innovation, being respectful of the environment when improving products, processes or services and helping increase quality of life. They have been involved in projects spread across many different technological sectors, all based on the core CRIC skills of integrating sensing and data gathering hardware with the software for processing and utilising the gathered data.

Why was it selected?

CRIC possess considerable experience in the area of software projects. Similar software/hardware integration projects that have been undertaken by CRIC include Vibratag, integrating wireless and intelligent sensor systems and Escola, integrating ultrasonic sensing equipment into an "on-the–fly" acquisition and monitoring system for the livestock industry. CRIC was willing to benefit from getting experience form the collective work on the analysis of data representing complex signals, as it could give them a better perspective for some of their undertakings involving such applications.

Partner 10 UoY

Business Activities
The Applied Electromagnetics and Electron Optics Research Group at the University of York (UoY) are considered world experts in the area of EMC compliance with over 400 publications in the last five years. The group's primary interest is the field of electromagnetics. Within this field they have a number of areas of interest and expertise that have evolved through their research over many years.

Why was it selected?
The Applied Electromagnetics and Electron Optics Research Group has experience conducting research on the potential human exposure to electromagnetic radiation through the UK government's Mobile Telecommunications and Health Research programme and on the design of wearable antennas for portable digital electronic systems. The group has also worked on diagnostic immunity measurements using the re-emission spectrum for the Radio Communications Agency, work for which it was awarded an IEEE Transaction paper prize in 2004. The Group also gained experience from involvement in an EPSRC-funded project for the detection of non-linear junctions in building structures associated with corrosion and antenna design. renowned expertise in the design of mobile telephone and wireless dosimetry equipment for estimation of SAR used in research programmes for the Department of Health (UK) for Mobile Telecommunications and Health.

Complementarity Between Participants

We identified and selected potential partners by screening to meet specific requirements such as technological ability, number of years in business and enthusiasm for new ideas and further, we conducted personal interviews in order to validate the potential of selected partners for a harmonised business relationship. The partnership thus formed provides the required manufacturing expertise in each area of the project without conflict or competitive interests. The partners each have a role in the completion of the various tasks and are fully involved in the task management of the project. Each partner will have a part to play in the commercial exploitation of the product and can provide the required input to guide the project to a successful conclusion.

As for the technical knowledge and component supply capabilities needed to develop and manufacture the detection system itself, we have assembled a specialist team to provide all the key component knowledge and manufacturing capabilities we need. All SME and OE proposers cooperated close with RTD partners to built

complete and robust system. Leading partner was INPOL, who was elected to lead partnership due to research and marketing experience. TTI who will be manufacturing transmit and receive antennas and user panels for system operation worked closely with INPOL and UoY who contributed in-depth expertise in developing TSCM equipment based on non-linear junction detection techniques. NATEL designs and supplies conditioning units, that can be used for high speed processing executing complex algorithms for different applications, and contributed much technical knowledge regarding the specification of conditioning and decision units along with developed algorithms and their practical integration into the detection system. SFTMND assisted in the development of the decision algorithm and database storing harmonic signatures, as well as control software for system operation. They are experts on complex high risk and real time software for IT and business applications, possessing extensive skills in building complex database and decision support systems. TSE was active in the field of designing and production of electronic components, assemblies and products with an expertise in cable manufacture and fabrication of hardware enclosures utilised their skills in fabrication and construction to build the arch hardware to incorporate the sensors and required wiring looms. The input from suppliers of system components was complemented by ETRONIC who have business relations with companies involved in monitoring and protection of people and property. Moreover ETRONIC is specialist in system integration and installation which makes them optimal partner for undertaking system installation and representation towards end users.

As a partnership of small firms in a huge potential European market of hundreds of billions of Euros, we appreciate that we lack the ideal range of distribution and customer contacts in the knowledge-reliant SME sector. To solve this problem, we invited to our consortium Authentix (AUTEN), a leader in authentication solutions for brand protection and fiscal recovery and Inicjator Sp. z. o. o. (INTOR) which is a law firm specialised in IPR protection. By using these two representatives of knowledge-reliant SMEs and professional services firms, our group of SME and OE proposers was able to acquire vital end-user functionality, application and installation knowledge to optimise our system development.

RTD organisations, i.e. INPOL, UoY and CRIC have been chosen by the SME group to provide them with extensive, and complimentary, competencies, resources and facilities for development of radio transmitters and receivers, microstrip antenna systems, advanced signal processing and algorithm development including expert systems and neural networks, sensors and identifiers, and their integration into complex signal acquisition and processing system. RTDs offered also experience and expertise in the development of electronic circuits and customised software for time critical applications. Finally, University of York, The Applied Electromagnetics and Electron Optics Research Group provided SMEs with expertise on EMF exposure, RF characterisation as well for EMC compatibility to help on validation of SafeTalk device through laboratory testing.

1.3. Work performed and end results including the description of methodologies and approaches employed

Apart from the official schedule based on Work Packages, the project lifecycle can be divided into the following stages:

1) Research
2) Development of hardware, software and arch mechanics,
3) Laboratory tests and integration
4) Population of database,
5) Validation,
6) Check against conformity to the standards,

Where the last activity coexisted with activities 2-5.

Research

Our first objective was to scientifically characterize, determine and enhance understanding and theoretical analysis of the models of harmonic responses of electronic devices (WP 1: Scientific Understanding and Review) To reach the goal of a semi-conductor junction, we analized excitations within an E-field (using Matlab and Mathcad tools) and obtained the signal which we expected could be detected by the receiving antenna. The simulations confirmed validity of the models and extended knowledge about harmonics generated by junctions and relations between them.

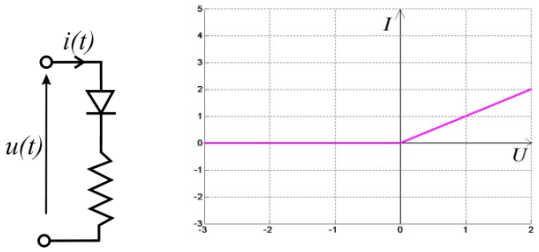


Figure 1. A sample model of the diode with resistor and the relevant I(U) curve.

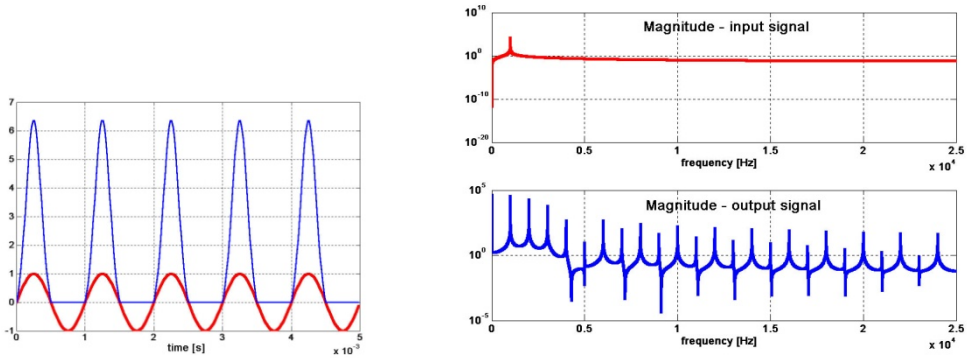


Figure 2. Sample results of simulations: In red – the voltage, being the input signal, in blue - the response of the sole diode element. On the left – time domain, on the right – frequency domain (magnitude only).

Next, we defined two possible solutions for NLJ detection, both novel and extending sensitivity of the detector beyond currently available values: the spread spectrum and synchronous detection technique. The spread spectrum and synchronous detection technique both make it possible to replace simple modulations with more sophisticated techniques. After further investigation, we found that the synchronous detection technique would be more useful due to better parameters which can be achieved, lower complication of the circuit and, finally, the lower price of the circuit.

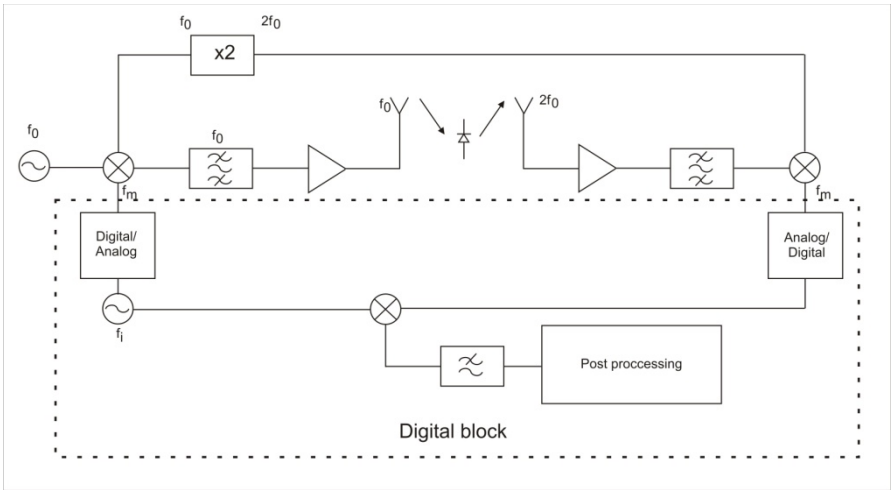


Figure 3. Block diagram of the developed NLJD with synchronous detection technique.

Simultaneously, the Consortium was working on the methods and algorithms for signal conditioning. At the beginning, multiple options were taken into account, including pre-processing with Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform and processing results of mentioned transforms with fuzzy logic algorithms and neural networks (Single Layer Perceptron, Multilayer Perceptron and Radial Basis Networks).

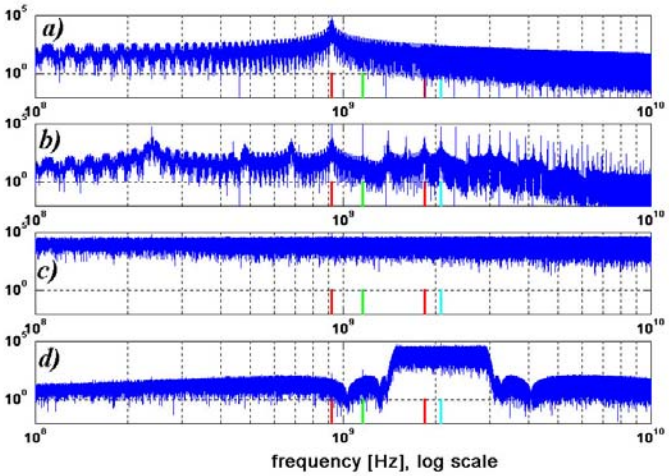


Figure 4. Example of the set of the Fourier magnitude spectra, for the experiment with parameter values described in the text below: a) for the s1 signal (after DSS and PSK), b) for the sd signal (after passing the diode), c) after adding the noise (34dB above the signal level), d) for the signal after BPF. The markers are: red for f1 and 2f1, green for f2 , cyan for f1 + f2 .

All these method constituted input for the next goal in the research, which was to achieve an enhanced understanding of the signal conditioning and matching of RF signatures vs decision time and probability. A set of devices representing various types and brands of standard equipment was prepared, which is likely to be used for spying action either directly or accompany such equipment. For these devices, several measurements were performed to investigate the possibility of detection and classification of such devices. The study has been performed with the use of the graphical and statistical analysis.

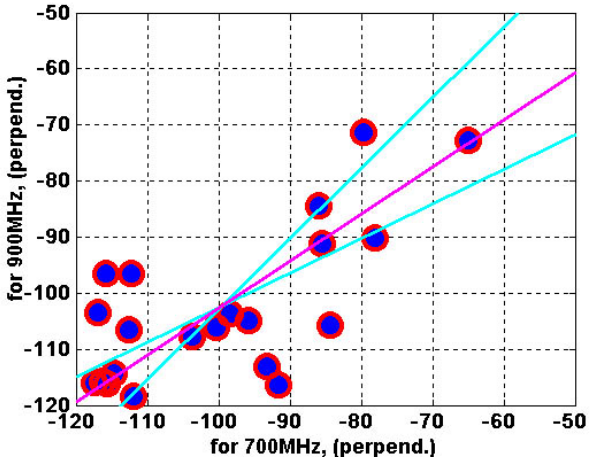


Figure 5. Maximum detected values at 2nd harmonic – comparison for two sources: 700MHz and 900MHz, and the same setup.

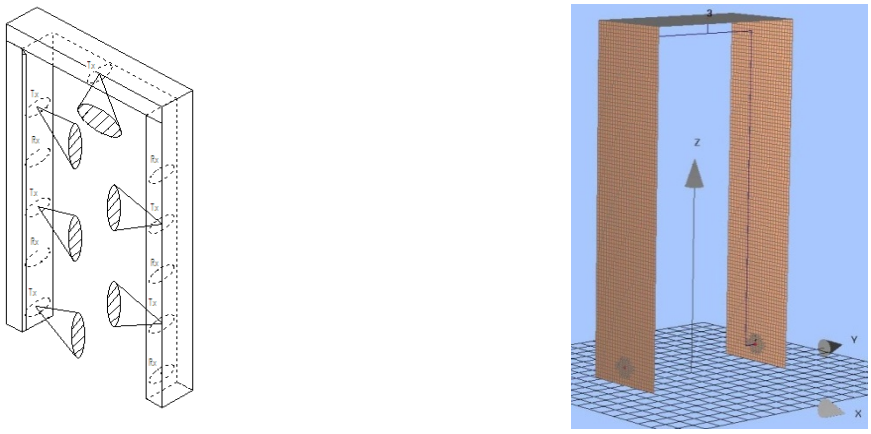
The conclusion was that results are repeatable and we should be able to create signatures for specific devices (not groups of devices in general). Finally, the preferred algorithms were: DFT for pre-processing and neural networks and Case-based reasoning (CBR) for classifying signals. Performed simulations showed that the envisaged probability of correct differentiation between metallic and semiconductor junctions at a level of 97% is possible, however the probability for correctly matching a signal to the stored signature will be at a level of about 80% and not 85% as initially assumed. It should be stressed that results obtained during validation were very close to the results originating from simulations, and at the final stage met initial assumptions. Apart from that the Consortium found that:

1) The basic functionality of the detector should show to the operator that the suspected object is on the target,

2) During investigations the Consortium found that clients are interested in the detection of suspected objects. Their classification is treated as an additional feature,

The consortium has therefore decided, that this difference between the original assumptions and obtained parameters during simulations was acceptable.

Finally, the Consortium aimed to enhance the understanding of the impact of geometrical arrangement of chips and junction characteristics as well as methods of emission of radiation on harmonic signatures. During this task we needed to identify the relation between the position of the target in space and arrangement of antennas which should guarantee the best possible illumination of the object with radiation and the highest level of returned signal for all possible orientations of junctions relative to the antennas. After tests performed in the reverberation chamber with different polarisation of the objects and after detailed analysis of the system's structure with narrow-band antenna vs. broad-band antenna, we decided that we would use broad-band antenna as the transmitting antenna and multiple narrow-band antennas for the receiver.



(a) (b)

Figure 6. a) Multiple narrow-band antennas for receiver, b) single broad-band antenna for transmitter.

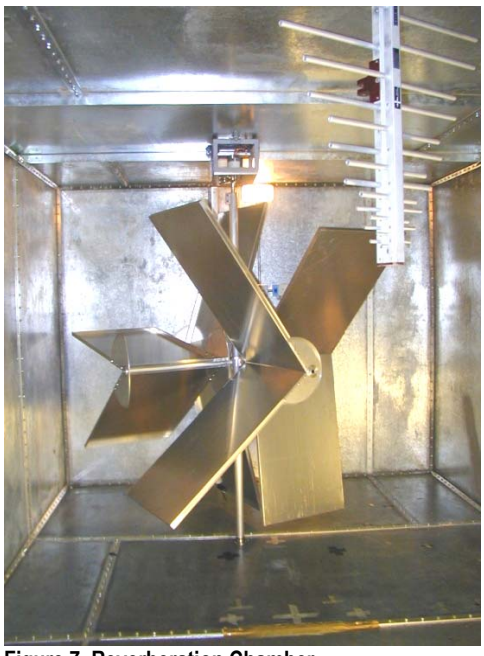


Figure 7. Reverberation Chamber

The next goal after extending the knowledge was to develop and build a prototype of the SafeTalk system in three separate areas: hardware, software and the mechanics of the arch.

Hardware development

To reach the goal in the form of development of hardware, we had to develop RF (microwave modules), antennas, acquisition module, user panel and integrate all these elements, which is shown in a schematic diagram of the developed NLJD in Figure 3.

The RF module consists of a low noise amplifier LNA, mixer, frequency synthesizer, voltage controlled oscillator detection circuit, power amplifier and a power supply unit. Low frequency electronics consist of controlled gain amplifiers, digital to analog converters and processor module. Schematics of the system are depicted in Figure 8 where PCB artworks are presented of the following figures below.

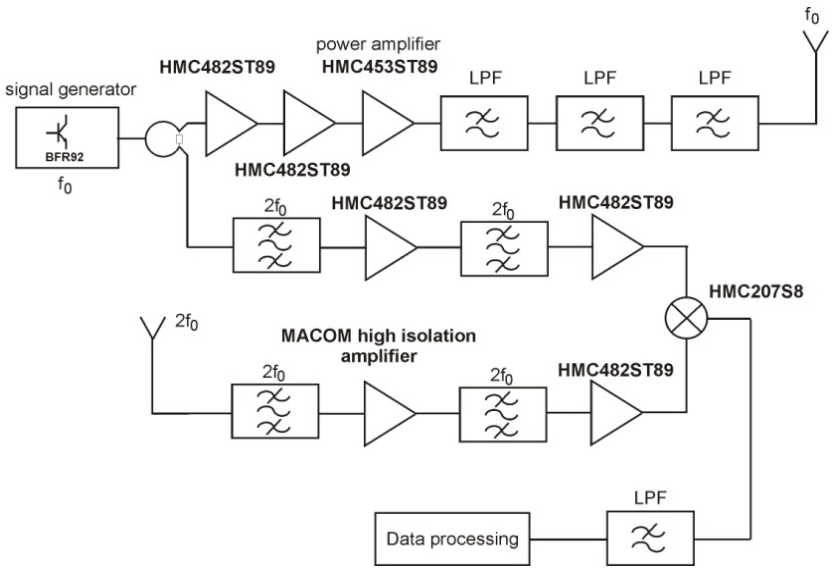


Figure 8. Schematic diagram of the developed nonlinear junction detection device with synchronous detection techniques.

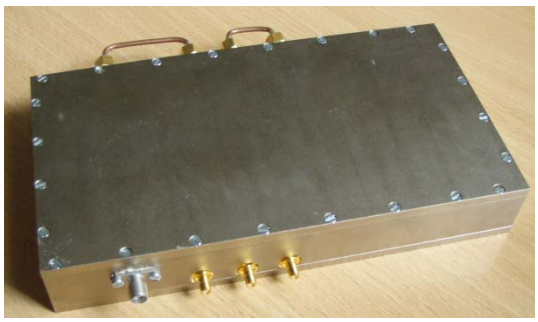


Figure 9. Picture of the developed receiver unit.

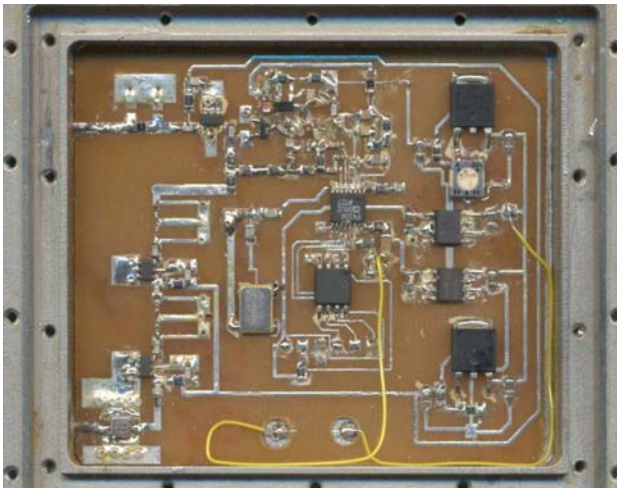


Figure 10. Picture of the developed frequency synthesizer and voltage controlled oscillator.

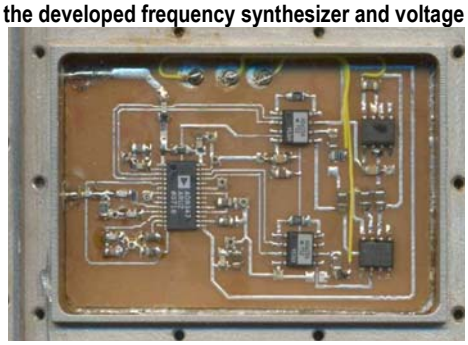


Figure 11. Picture of the developed microwave mixer.

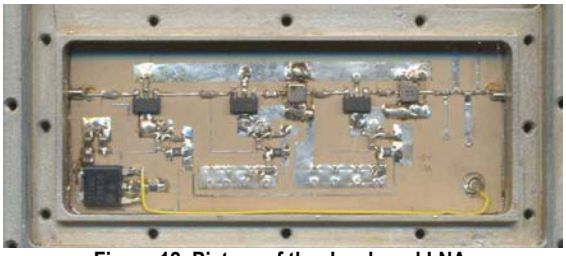


Figure 12. Picture of the developed LNA.

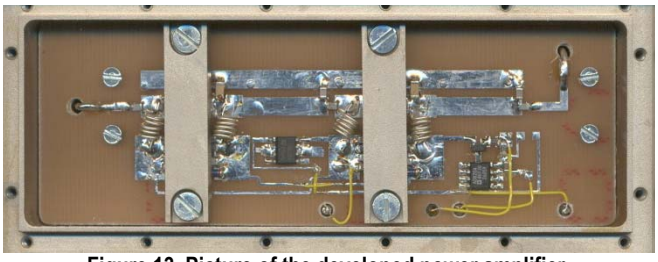


Figure 13. Picture of the developed power amplifier.

Figure 14. Picture of the developed low-pass output filter.

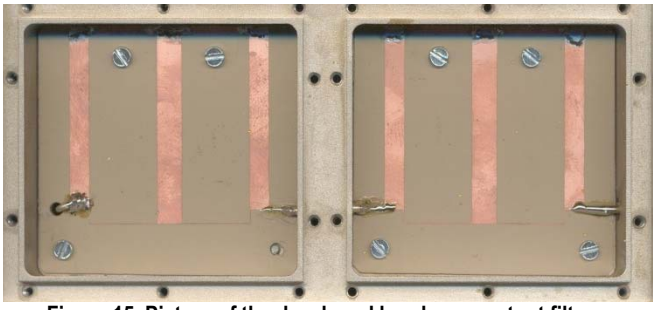


Figure 15. Picture of the developed band-pass output filters.

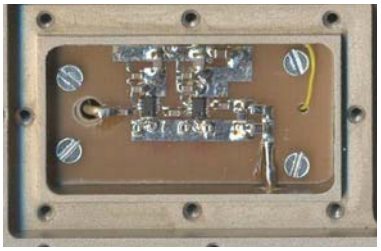


Figure 16. Picture of the developed driver for the power amplifier.

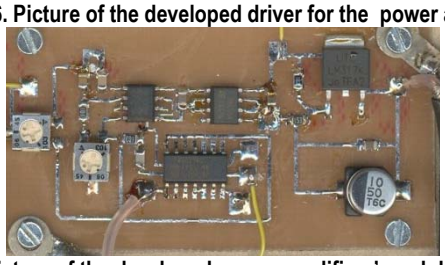


Figure 17. Picture of the developed power amplifiers' modulation circuit.

As mentioned above, after several investigations and analysis of system performance, the Consortium decided about the final shape of the antenna system for the SafeTalk project, which constitutes:

1) One, broad-band antenna for transmitter in the shape of long line,
2) Several (in the commercial application at least 8) multiband antennas for reception of radiated signals.

The picture below depicts an example of two receiver antennas together with a long line antenna for transmitter.

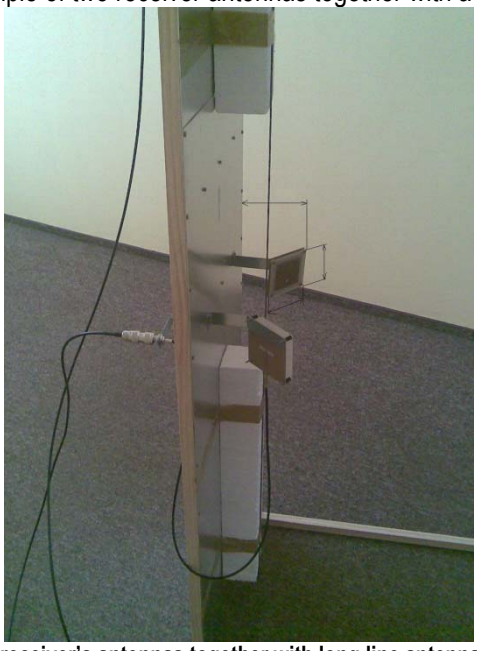


Figure 18. Two receiver's antennas together with long line antenna for transmitter

Multi-band antennas were used for the receiver which are widely used in today's electronics since they offer a reduced size and lower manufacturing costs of modern electronic equipment. In this solution, two separate antenna arrays consisting of broadband monopoles as radiating elements are connected together with the use of a frequency diplexer. Figure 19 shows a layout of the designed antenna element. Calculated return losses and isolation of the designed antenna are presented in Figure 20. Figure 21 presents a photograph of the designed antenna in which two separate patches integrated within one structure are visible. The usefulness of the proposed antenna in application in a NLJD has been evaluated and a good detection capability has been obtained in comparison with two separate standard microstrip patches.

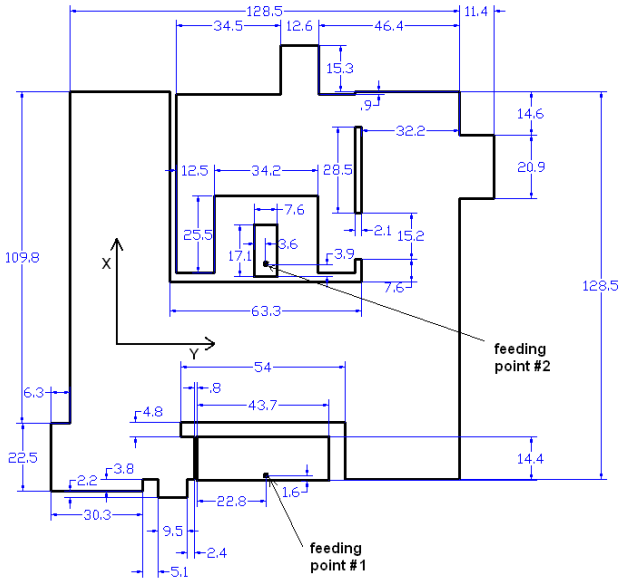


Figure 19. Layout of the receiver's antenna

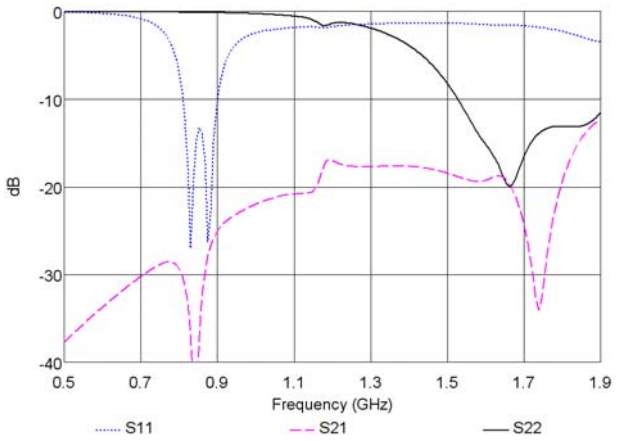


Figure 20. Calculated S parameters of the designed antenna

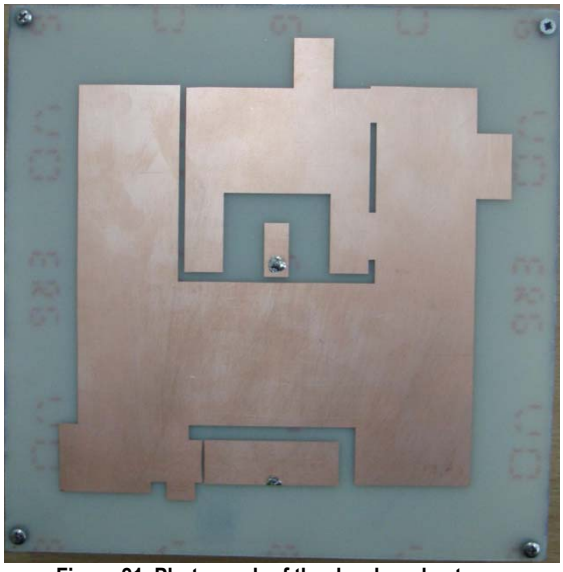


Figure 21. Photograph of the developed antenna

For the acquisition module we used the HSB-1616USB-HS acquisition board as a platform acting as an analog to digital converter and front end in our system. It allows for efficient data processing with flexibility coming from programming in high level language, i.e. C++.

Figure 22. The USB-1616HS-2 unit.

To communicate with user without need to use a mobile computer, a dedicated user panel was designed. Messages by the user panel are communicated only with the use of LCD display to inform the operator that some kind of electronic equipment has been detected on the target.

The developed control panel consists of an LCD display having 4x16 characters six control buttons LED signalization and a sound signalization (buzzer). The developed module allows for reading the present level of the detected signal, setting threshold value for the sound alarm, changing the operating power and duty factor for the transmitted signal. The system utilizes AVR ATmega 644 microprocessor from Atmel.

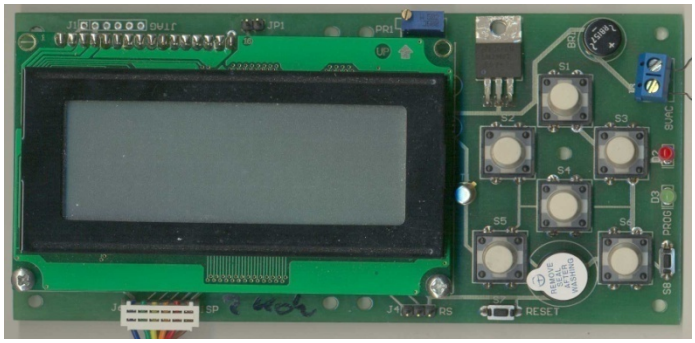


Figure 23. User Panel.

Arch's mechanics

The next goal was to develop an arch structure according to the project assumptions. During the scope of the project two prototype units were developed: a laboratory (Figure 24) and a commercial prototype (Figure 26).

Figure 24. Prototype of arch.

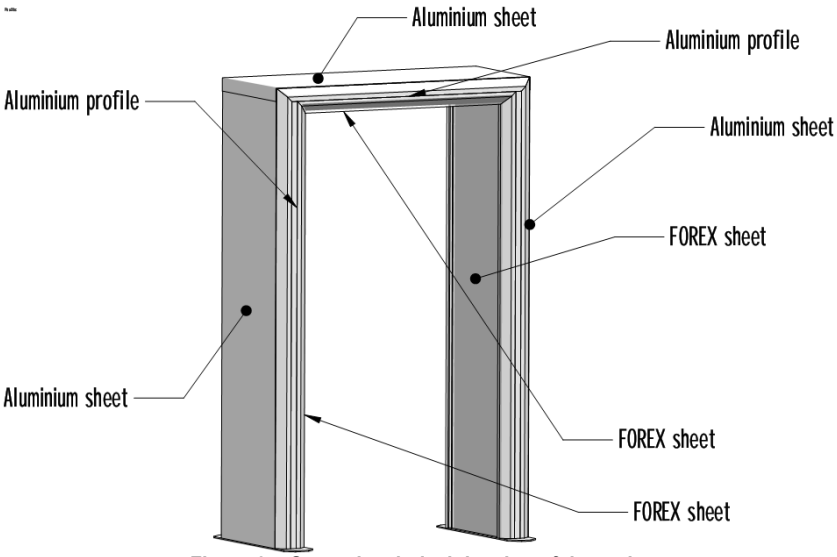


Figure 25. General technical drawing of the arch

Figure 26. Assembled arch ready for operation

The developed hardware was integrated and tested in the laboratory before integration in the first test site.

Figure 27. Tests of the SafeTalk system in the laboratory Software development

Software

The next challenge was to develop the software for the system. The developed solution is composed of different modules – see the picture below.

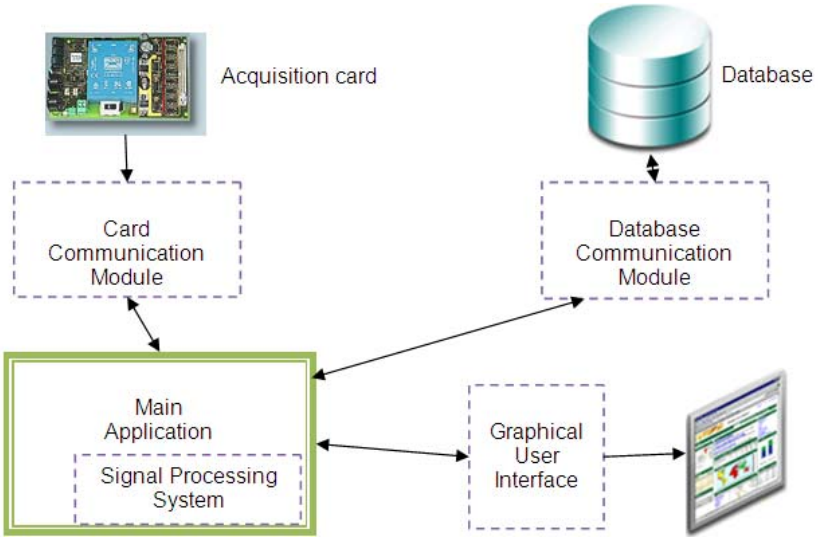


Figure 28. Structure of the SafeTalk software

The diagram above shows an overview of the software system classes architecture. The main module (in the bottom left) is the central point in this system getting information from some modules and sending other information to other modules after being processed in the built-in signal processing system. The diagram below shows the diagram of classes of the software system.

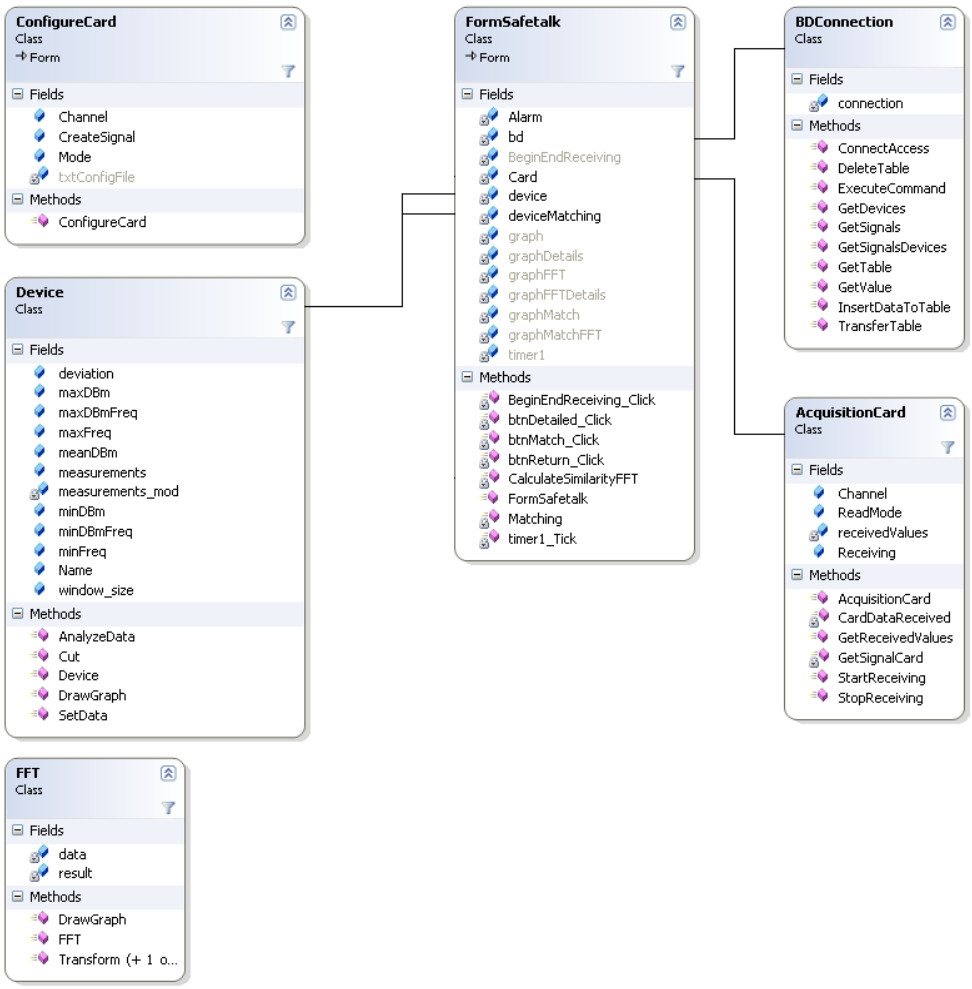


Figure 29. UML diagram of SafeTalk classes

Below is a snapshot of a sample screen from the application – setup of classification method.

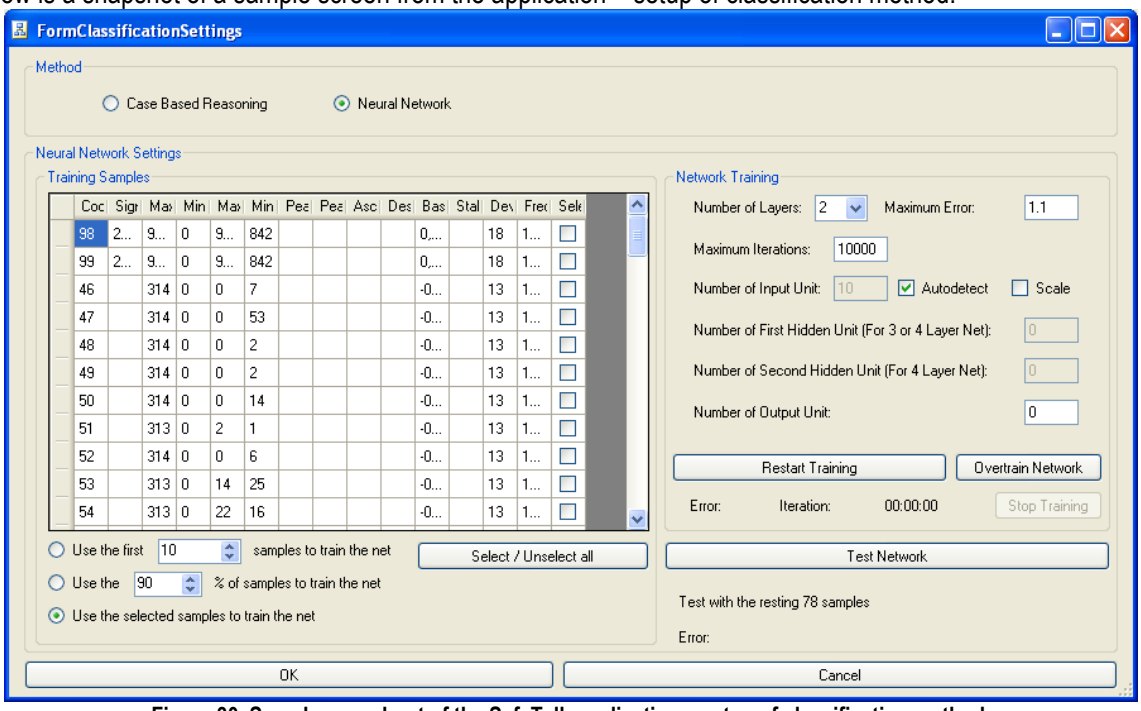


Figure 30. Sample snapshoot of the SafeTalk application – setup of classification method.

To complete the system of user notification, we had to complete a task related to the development of the control unit and user panel. Apart from the software module in the main application allowing for control and maintenance (see snapshot below) the independent user panel was developed – see above in section Hardware.

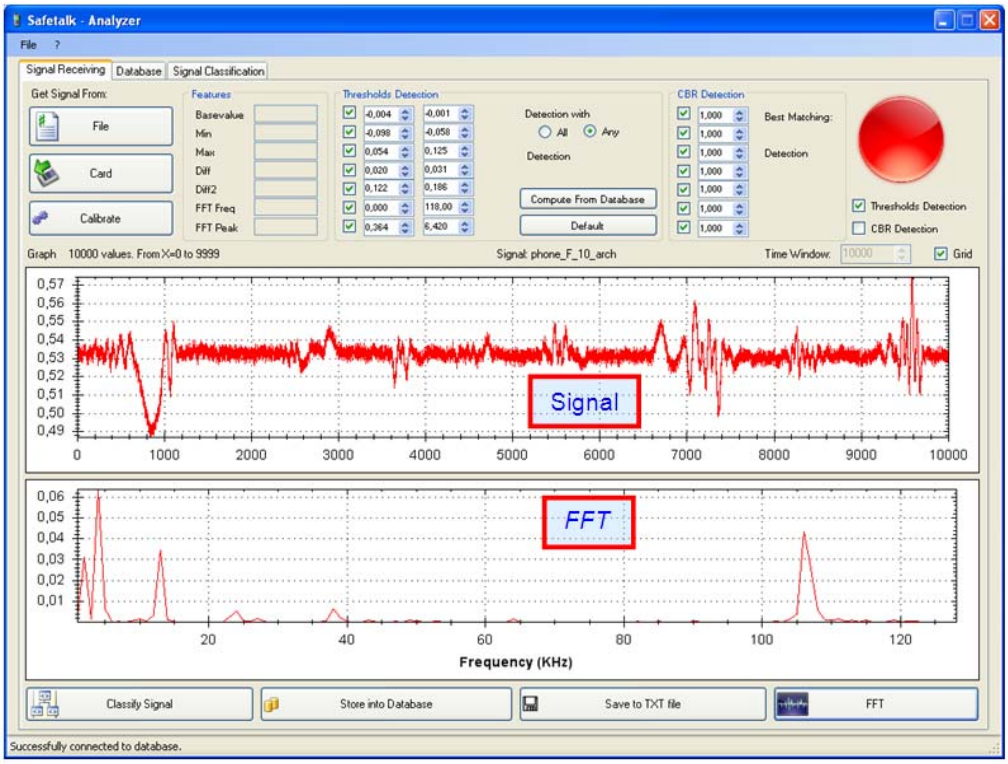


Figure 31. Sample snapshoot of SafeTalk application – information panel.

After successful tests on algorithms and methods of harmonic response analysis, the Consortium developed software for the SafeTalk system. The developed application allows for:

1) Calibrating the system,
2) Storing harmonic signatures,
3) Training neural network,
4) Detecting electronic devices,
5) Classifying electronic devices according to the content of the SafeTalk database.

Integration

After development of the software, all components were integrated into a prototype arch system. The Consortium integrated all elements developed during WP1, WP2 and WP3 into a complete SafeTalk system and installed it in at the premises of Innowacja Polska– see the picture below.

Figure 32. Picture of the integrated SafeTalk system

The integrated system was initially tested and data analyzed by the partners. The first results were quite good, however optimal parameters were obtained during validation after adjustment of system's settings.

Population of Database

During population and validation of the database library, the Consortium acquired a big number of test signals for the development of the software system (up to 1500). Within the scope of the project, the database was populated with 26 harmonic signatures of the devices which can be used as eavesdropping units:

1) Eavesdropping device no. 1 (camera inside the pen, readily available in Poland and elsewhere)
2) Eavesdropping device no. 2 (amateur spying kit)
3) Eavesdropping device no. 3 (miniature GSM spy kit)
4) Eavesdropping device no. 4 (miniature eavesdropping device)
5) Eavesdropping device no. 5 (miniature eavesdropping device)
6) Mobile Recorder 1 (PHILIPS)
7) Mobile Recorder 2 (PENTAGRAM)
8) Mobile Recorder 3 (SAMSUNG)
9) Mobile Recorder 4 (PANASONIC)
10) Mobile Recorder 5 (CREATIVE)
11) Mobile Recorder 4 (OLYMPUS)
12) Cell phone 1 (Sony Ericsson)
13) Cell phone 2 (Sony Ericsson)
14) Cell phone 3 (Sony Ericsson)
15) Cell phone 4 (Nokia)
16) Cell phone 5 (Nokia)
17) Cell phone 6 (Nokia)
18) Cell phone 7 (LG)

19) Cell phone 8 (LG)
20) Cell phone 8 (Motorola)
21) Cell phone 9 (Motorola)
22) Digital Camera 1 (Sony)
23) Digital Camera 2 (Sony)
24) Digital Camera 3 (Panasonic)
25) Digital Camera 4 (Panasonic)
26) Digital Camera 4 (JVC)

Here is the picture of an sample eavesdropping device, which has been designed intentionally for the purpose of spying and which was incorporated in our database.

Figure 33. Eavesdropping device no. 1 (camera inside the pen, readily available throughout Poland and other countries)

Validation

The last Work Package related to the development cycle was listed as Work Package 5 and was entitled 'Validation of the prototype system'. The system was validated in two independent test sites:

1) EC Electronics (member of the consortium) in December and January,
2) EC Micro Tech (subsidiary of Innowacja Polska) in January and February.

Both companies are committed to keeping their IP confidential and making it inaccessible to unauthorized persons. EC Electronics is involved in carrying out many projects related to military applications, including a system for navigating missiles. Personnel of EC MicroTech was involved in projects for the European Space Agency, and the company is in the process of negotiating another project under the PECS funding mechanism. Validation was performed in two modes:

1) simulated silent operation,
2) checking of visitors.

In the first mode (simulated silent operation) randomly selected employees carried a randomly selected eavesdropping device through the gate once a day at a randomly selected hour. In the case of the test which relied on checking visitors, we enquired with people visiting both companies if they agreed to be checked with SafeTalk system. About 65% of the visitors agreed.

In all tests (silent mode in EC Electronics and visitor check at EC MicroTech) we obtained a rate of detection of electronic devices at level of 96-97%. In the test designated as the "silent mode", which was performed at EC Electronics headquarters, the level of the detection of type of devices was 80%. Following these tests, part of the validation system was adjusted and trained additionally. As a result, during the "silent mode" test performed in EC MicroTech, the level of successful recognitions of the device type was 86,67%.
The obtained results show that project objective has been reached. However we need to stress that obtaining good results by the system is strictly connected with proper installation and system adjustment to the conditions present at a given installation location.

Conformity to relevant Standards

Simultaneously, test and validation activities for verifying conformity to standards were performed. In addition to the various EMC Directive standards, the R&TTE Directive lists a number of human exposure standards to ensure that products comply with EU safety regulations according to Council Directive 73/23/EEC. Council Recommendation 1999/519/EC provides basic restrictions and derived reference levels for exposure of the

general public in the areas where they spend significant time based on the ICNIRP Guidelines. The relevant product specific standard for the NLJD is EN 50364:2001 for Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications. This standard references the generic standard EN 50357:2001 for specific techniques to demonstrate compliance.

SAR measurements made on the short antenna and predictions made using the modelling have good agreement and both indicate an absorbed power density for an input power of 2W (continuous) just below the safety levels. Further modelling carried out on the full sized model indicates that the field levels close to the antenna are no higher than those for the short antenna which indicates that the absorbed power will also be within the limits. The field levels generated by the arch (in the commercial version) at the fundamental frequency should be lower than the limits at distances of greater than 40mm from the transmission line radiator. If higher powers are to be used to increase the sensitivity of the system then it will be necessary to pulse the power to stay within the time averaged limits.

To promote the results of the project, the Consortium actively worked on innovation related activities, to broadcast the benefits of the developed technology and knowledge beyond the consortium to potential industrial user communities (by tradeshows, conferences, papers, press articles). Also the knowledge from the RTD performers to the SME participants was transferred to enable them to rapidly apply and embed the technology onto specific products.

Conclusion
The main conclusion at the end of the SafeTalk project is that all the project's goals were reached, and a prototype of the SafeTalk system is ready for the next stages of commercialization.

To promote the results of the project, the Consortium has actively worked on innovation-related activities, to broadcast the benefits of the developed technology and knowledge beyond the consortium to potential industrial user communities (by tradeshows, conferences, papers, press articles). Also the knowledge from the RTD performers to the SME participants were transferred to enable them to rapidly apply and embed the technology onto specific products.

1.4. Elaboration on the degree to which the project's objectives and goals were reached

The scientific objectives of the project involve the extension to current knowledge of:

1. Characterisation mechanisms for definition, possible detection and analysis of device harmonic signatures incorporating multiple non-linear junctions, including required RF field strengths, modulation schemes for a probe signal and exposure time required, and the optimal set of harmonic signature characteristics (amplitudes of harmonic signals, phase shift and group delay) that can be used to constitute harmonic signature of a device discriminating false non linear junctions and providing sufficient information for device classification (OBJECTIVE MET).
2. Issues of RF signal acquisition in relation to multiple space diverse receivers including optimal antenna design, receiver sensitivity, selectiveness of filters, measurement time and complexity required, repeatability and robustness in the face of interference or ability to reject interference (OBJECTIVE MET).
3. Estimation of SAR in the limbs and torso of a person at the nominal operating distance and the spectrum regulatory framework that the devices will have to exist within (OBJECTIVE MET).
4. Harmonic signature analysis using fuzzy logic paradigm for classification purposes and neural network for matching to patterns stored in database library populated for different types of electronic surveillance devices (OBJECTIVE MET).

By meeting the scientific objectives the project is expected to give rise to the following technologies:

- A method for reliable detection and characterisation of harmonic answers from devices incorporating non-linear junctions (OBJECTIVE MET)

- An apparatus for classification and matching harmonic signatures on the basis of harmonic answers from electronic devices (OBJECTIVE MET).

The overall technical objective is to produce a commercially viable system, at a price of €7,000, for detection and identification of 85% of available electronic surveillance equipment, passing through a doorway into a protected room, laboratory or workspace. In addition, **specific technological objectives** need to be satisfied to enable the system to:

1. **Permanently detect the presence of any electronic device** passing through an arch of a volume of 4m^3 through the RF illumination of the concealed device using a deliberately modulated probe signal and subsequent analysis of a conjugated harmonic response generated by the non linear junctions in the device. The envisaged probability of recognition of a semiconductor junction will be 97% (OBJECTIVE MET).
2. **Analyse the RF harmonic responses** and accomplish signal processing for device detection and identification based on an average walking speed of 5 km/h. The technical objective is to develop a **signal conditioning unit** performing demodulation, as well as FFT analysis for discrimination of 2nd, 3rd and higher order harmonics, as well as known clock signals capable of providing within 100ms operational time an information vector necessary for building harmonic signature (OBJECTIVE MET).
3. **Ensure compliance to EMC regulations** and health & safety issues. Specifically, the worst case SAR (Specific Absorption Ratio) must meet the ICNIRP guidelines and comply with the new EU directives on safe limits of RF exposure by developing **microstrip antenna systems**, the **RF transmitter** and **receiver** that will in implemented into the **plastic arch structure**, thus limiting the sensing distance to 1 m (OBJECTIVE MET).
4. **Store up to 100 RF harmonic signatures of known electronic surveillance devices** within a specially designed reconfigurable database interacting with the decision unit to ensure that at least 85% of the various types of electronic eavesdropping devices. The first 25 of the 100 harmonic signatures will be loaded onto the database within the timeframe of the project and using the prototype arch produced by the project (OBJECTIVE MET).

Conclusions:

1) During our project all technical objectives were met,
2) All WPs and Tasks were successfully completed.
3) We have completed the project with a laboratory prototype of the detector of eavesdropping devices with parameters (technical and economical) which of interest to potential end-users.

1.5. The achievements of the project to the state of-the-art

The search for eavesdropping devices has been conducted up until now by using portable devices. The portable devices are only able to detect a potential eavesdropping device by costly systematic sweeping of potentially compromised areas by expert users. On average (for a two floor building of approximately 20 rooms), the cost to the SME for the sweep service is €4,000 each time[1]. In fact, private investigators claim that organisations are paying up to €15k to have their premises checked to keep sensitive information under wraps[2]. **No technology has existed until now that could be installed into a room permanently, to proactively scan to make it permanently and continuously safe to talk**, whilst being able to detect devices and determine their nature and level of security threat as a listening device or video camera.

Such a "preventative" device is now available to SMEs involved in providing hi-tech and professional services, at a price level (of around €7,000) that will allow to **create a "Safe-Talk" room, laboratory or work space in** a cost-effective way.

The key advantages over currently used systems for motion detection are: **continuous operation on human targets** (as one of primary objectives), **low cost** (in contrast with the methods being currently in use)**, high reliability and precision, additional functionality** (recognition of type of the object) and **possibility to integrate with a door frame**. In order to achieve that we had to overcome the primary technical barriers. We achieved this by:

[1] Quotation obtained from Audit-Com, counter surveillance agency
[2] Blue chip firms find bugging is now big business, Scotsman 2003

- Permanent detection of the presence of any electronic device passing through an arch of a volume of 4m3 through the RF illumination.
- Extending knowledge in the area of RF harmonic responses and accomplishing signal processing for device detection and identification
- Development of a signal conditioning unit performing demodulation, as well as FFT analysis for discrimination of 2nd, 3rd and higher order harmonics,
- Storing up to 100 RF harmonic signatures of known electronic surveillance devices within deliberately designed reconfigurable database.

The impact of the project on the industry sector

We hope to help protect and sustain the competitive position of the community of over 750,000 **innovative, hi-tech SMEs**, recognised by the EC as being the hub of innovation and involved in leading edge research in Europe[3]. Whilst prolific generators of new science and technology (120,000 new European Patent applications every year), small, often micro, hi-tech SMEs are vulnerable to theft of their Intellectual Property (IP) and potential differentiation in their marketplace. In Europe, the damage to competitiveness and lost sales due to IP theft is put at €120Bn annually[4], and it is estimated that the specific impact on hi-tech SMEs is around €35Bn pa[5] which whilst a small proportion of the total EU losses, represents a large proportion of the hi-tech SME sector turnover, which is €870Bn pa[6]. The IP possessed by hi-tech SMEs represents 82%[7] of their business value, and its protection is perceived by them as being critical to their longer term sustainability and survival. Annually, IP theft is estimated to cost the typical hi-tech SME around €34,000 pa[8].

The losses incurred by knowledge theft impact on other sectors too. Commercially, critical knowledge need not necessarily be Intellectual Property it may simply be privileged or confidential information. The protection of this form of information is vital to the competitiveness of **Professional Services firms in Europe**, such as the 120,000 SME law firms, 250,000 SME accountants and 200,000 SME insurers. The information, requiring protection in these types of SME can be used by others to commit a range of fraud offences from investment fraud to embezzlement to false insurance claims and insurance certificate production. In the absence of statistics annual loss in specific sectors is estimated to be in excess of €2.5Bn for SME law firms, €3.5Bn for SME accountants and €6.5 billion for SME insurers respectively[9].

The third community of SMEs we hope to help are the European manufacturers of counter-surveillance equipment themselves. Electronic Eavesdropping Detection Equipment falls into the 'other electrical security systems and products' category in Freedonia's Security Reports. The January 2003 report states "the world market for 'other electronic security systems and products' is projected to log double-digit gains through 2006, rising 16% per annum to €3,43M, of which €1,06 will be spent in Europe". Another market which can also give clues to the size of the Eavesdropping Detection market is the Information Security market which was worth €11.4Bn in the EU in 2003[10]. The European market for both surveillance and counter-surveillance equipment is dominated by external suppliers. It is estimated that European suppliers posses only 30% of the market share in this specific sector in the EU[11]. The domination of large North America suppliers generating most of advances and innovations in the field of counter-surveillance equipment which is primarily caused by higher awareness of loss related IPR and confidential information theft, negatively influences on European SEM suppliers. One of the ways for EU suppliers to increase their share of the global markets is to develop lower cost and reliable devices

[3] EURAB report on SMEs and ERA, 2004
[4] The Federation Against Copyright Theft, FACT website March 2004 - £9Billion (UK) (Converted to Euros and scaled up by ten for EU25)
[5] The ABCs of Intellectual Property Protection, http://www.csonline.com/fundamentals/abc_ip.html
[6] Based on data from Observatory of European SMEs 2002 / No 6 High-tech SMEs in Europe
[7] Scientific Report on KI in Practice, Data Collection & Analysis; results of GROWTH Project No G1RD-CT-2002-00700
[8] Based on data from SME in Focus, Observatory of European SMEs 2003
[9] Based on scaled up data from The Association of British Insurers
[10] (2003) World Security Products Industry Study: The Freedonia Group
[11] The 2003-2008 World Outlook for Security and Safety Equipment, ICON Group International Inc.

to help the large volume markets represented by the two communities above to protect themselves against IP and knowledge theft.

The long term impact of the project is different for each SME. Specific advantages for each are as follows:

- NATEL: The company expects to supply reconfigurable modules or the upgraded algorithms to the device integrator in the supply chain.
- SFTMND: The company expects to broaden portfolio of their services by building up new expertise in using their IT knowledge on developing databases and algorithms. Also they expect to provide, maintain and upgrade software for the SafeTalk system.
- TTI: The company expects to supply microstrip antennas and control panels to the device integrator.
- ETRONIC expects to expand their business by offering the SafeTalk system to the High Tech Innovative SME market as well as benefiting from facilitating installations.
- TSE: The company expects to expand their business by supplying components of arch architectures.
- INTOR: They expect to benefit from disseminating the SafeTalk system to communities of SMEs expressing the need for permanent IP protection in Poland.
- AUTHEN: They expect to benefit from advertising the SafeTalk system among communities of SMEs with needs for permanent IP protection in the UK.

Through participation in the project, each SME increased in competitiveness going beyond the opportunity to offer a specific component or service related to the markets identified, but also including the transition towards joining the new knowledge-based economy with partnered exploitation of the IPR created by the project and owned by the SME proposers. Furthermore, the provision of new knowledge differentiators to the sectoral community of SMEs also provided opportunities for the Core group of SMEs to increase their perceived value to their customers as strategic supply partners with innovative product development capabilities.

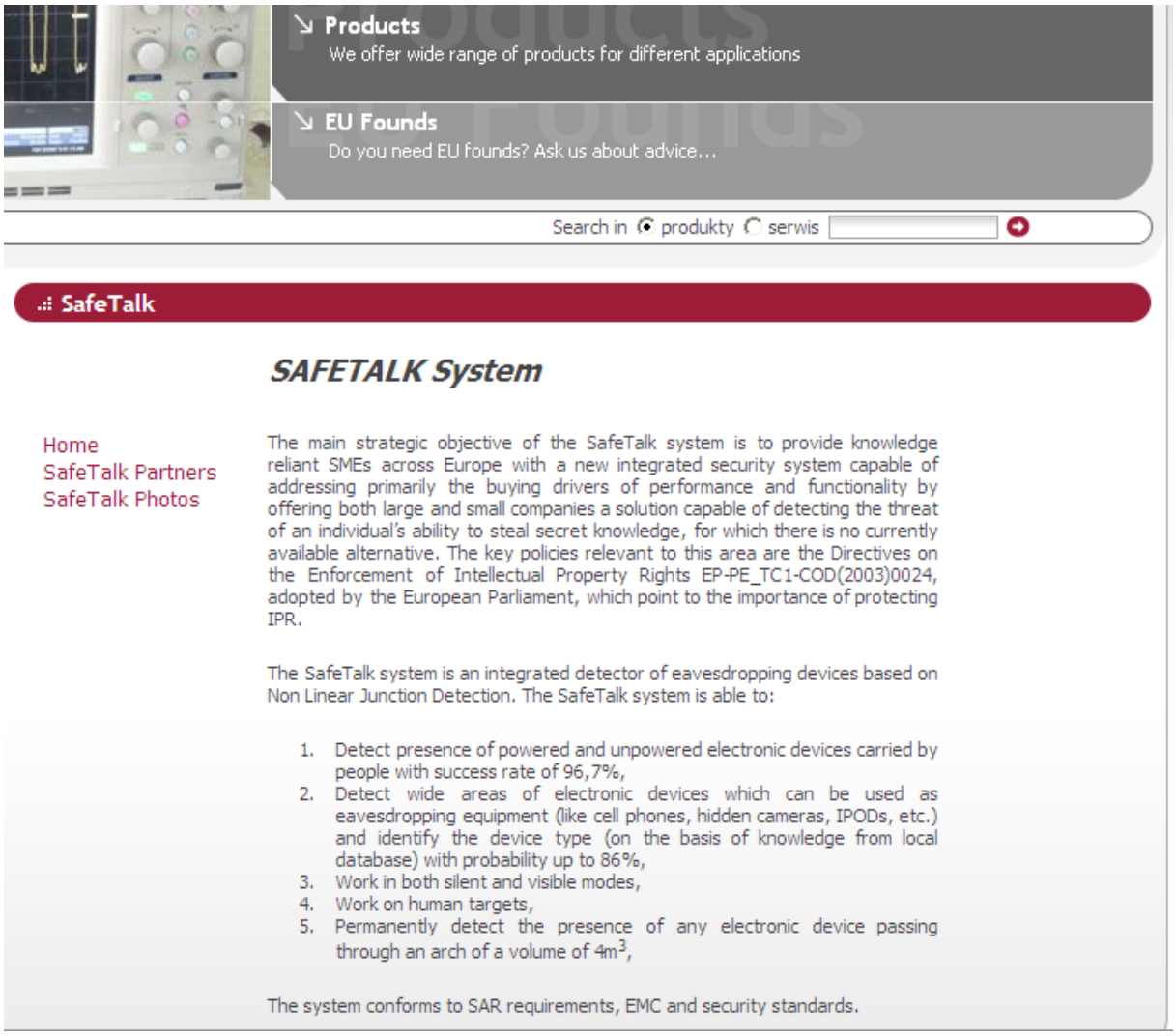
1.6. A project logo.

The project logo is presented below. It will also be used to promote the products.

Figure 34. SafeTalk Logo.

1.7. A reference to the project website.

The project's website can be visited at the following address: http://www.safetalk.eu. Provided below are snapshots of sample pages from that website.



EU Founds

Do you need EU founds? Ask us about advice...

Search in produkty serwis

SafeTalk Photos

Fig. 1 SafeTalk System

Fig. 2 SafeTalk System

...::Back::...

Section 2 – Dissemination and use

This section has been prepared following the published guidelines that it should only contain results that the Consortium is ready to publish and has already obtained sufficient protection for the IPR involved.
The main strategic objective of the SafeTalk system is to provide knowledge reliant SMEs across Europe with a new integrated security system capable of addressing primarily the buying drivers of performance and functionality by offering both large and small companies a solution capable of detecting the threat of an individual's ability to steal secret knowledge, for which there is no currently available alternative. The key policies relevant to this area are the Directives on the Enforcement of Intellectual Property Rights EP-PE_TC1-COD(2003)0024, adopted by the European Parliament, which point to the importance of protecting IPR.
The SafeTalk system is an integrated detector of eavesdropping devices based on Non Linear Junction Detection. The SafeTalk system is able to:

1) Detect presence of powered and unpowered electronic devices carried by people with success rate of 96,7%,
2) Detect wide areas of electronic devices which can be used as eavesdropping equipment (like cell phones, hidden cameras, IPODs, etc.) and identify the device type (on the basis of knowledge from local database) with probability up to 86%.
3) Work in both silent and visible modes,
4) Work on human targets,
5) Permanently detect the presence of any electronic device passing through an arch of a volume of 4m^3,

The system conforms to SAR requirements, EMC and security standards. The price of the basic configuration of the system is at level of 4000 EUR. Below you can see the SafeTalk system in operation.