REWARD
Real Time Wide Area Radiation Surveillance System

PROJECT FINAL REPORT

Grant Agreement number	**284845**
Project acronym	**REWARD**
Project title	**Real Time Wide Area Radiation Surveillance System**
Funding Scheme	**Collaborative Project (FP7-SEC-2011.1.5-1)**
Period covered	**December 2011 to November 2014**
Coordinator Name *Organisation*	**Dr. Manuel Lozano** **Consejo Superior de Investigaciones Científicas (CSIC)**
Tel *Fax:* *E-mail*	**+34 935 947 700** **+34 935 801 496** **Manuel.Lozano@csic.es**
Project website address	**www.reward-project.eu/**

Change History

Version	Date	Status	Author (Benef.)	Description
0.1	12/12/2014	Draft	Alberto Fernández (S&C)	Initial contents
0.2	12/01/2015	Draft	Carlos Figueiredo (EDI) Alberto Fernández (S&C) Elena Turco (S&C)	Security Framework Middleware Exploitation
0.3	14/01/2015	Draft	Carla Conti (VCT)	Decision support system
0.4	15/01/2015	Draft	Carla Conti (VCT)	Validation
0.5	16/01/2015	Draft	Elena Turco (S&C)	Section 4
0.6	16/01/2015	Draft	Michael Fiederle (XIE)	Sensor
0.7	19/01/2015	Draft	Celeste Fleta (CSIC)	Sensor, scenarios
0.8	19/01/2015	Draft	Carlos Jumilla (CSIC)	tag
0.9	20/01/2015	Draft	Elena Turco (S&C)	Minor changes & updates Version for internal revision
1.0	22/01/2015	Final	All members	Final document

Table of Contents

List Of Figures

List Of Tables

1 Executive summary.

This document summarizes the project REWARD after its finalisation. The project started on December 2011, and has finalised on 30th November 2014. The authors have tried to use non-scientific naming and explanations as much as it was possible hoping the explanation can be understood by a wide type of audience.

The reader will find the context of the project in section 2. This section explains the motivations of REWARD and the objectives finally accomplished. The main results and foregrounds are detailed in section 3. The section 3 starts with a global overview of REWARD system, where the reader will understand all system components and how they interact to bring the REWARD system function. After this introduction, each main component of REWARD system is further explained. The explanation starts by introducing the target scenarios of REWARD. Those scenarios were the base for the development of REWARD specifications. After this explanation, each component, starting from sensors up to high-level application software components is explained. This section finishes summarizing the field validation of the overall system. For each of the subsections, results and foregrounds are highlighted.

2 REWARD context and objectives summary

In the last decade, an increasing risk has arisen at world level coming from the unknown location of nuclear and radioactive sources that were mainly fabricated in the former Soviet Union and that, since its disintegration, have not been as strictly controlled as prior to the disintegration. Added to this other states such as Pakistan, who also have their own nuclear material, are known to have been causing concern to security intelligence agencies such as those of the United States, the United Kingdom and Russia who are not 100% sure that Pakistan can keep control of all such material. In the period 1993-2009, the IAEA Illicit Trafficking Database (ITDB) [Itd10] confirmed a total of 1,773 incidents involving nuclear materials, reported by the participating States and some non-participating States. Of these confirmed incidents, 351 involved unauthorized possession and related criminal activities, fifteen of them involving highly enriched uranium or plutonium. Five hundred incidents involved reported theft or loss (in 45% of the cases the lost or stolen materials were never recovered), and 870 incidents involved other unauthorized activities and events.

As an example, in 1994 almost three kilograms of highly enriched uranium were seized from nuclear smugglers in the Czech Republic. In year 2007, one kilogram of the same material was seized in Slovakia, dramatically illustrating the breakdown in controls over weapon-usable nuclear material in the former Soviet Union (the suspected source of the material) and making clear that terrorist groups are seeking to build a nuclear device.

Another type of radioactive threat, more common, is the loss or abandonment of equipment containing radioactive materials such as medical radiotherapy sources, or industrial radiology or densitometry systems. In some of the cases, as the ITDB report quotes, the sources are recovered. Unfortunately, this is not always the case, and this can have disastrous health, social and economic consequences. The Goiânia accident in Brazil in 1987 is one such shocking example, in which four people died, 249 were seriously contaminated and more than 100,000 were called for monitoring when an old nuclear medical source was scavenged from an abandoned hospital and released into the public environment[1]. Another more recent example of stolen radioactive material occurred in Mexico in December 2013, when a truck containing Cobalt-60 was stolen and then found in an empty lot close to an agricultural town. Fortunately, there were no people where the source of radioactivity was and only the person involved in opening the shielded box were in very great risk of dying.

Nowadays radioactive sources are widely used in medicine, industry and agriculture. Their security has become a growing concern, particularly the potential that such a source could be used as a radioactive dispersal device or “dirty bomb”. The number of potentially dangerous nuclear transports is still high, as demonstrated by trucks containing radioactive material stopped on European roads (Austria, May 2013 – Italy, July 2013). Calls are so growing for more routine radioactive screening. Because of the high risk to citizens’ health if these radiation sources are deliberately or accidentally

[1] A. Ansari, “Radiation Threats and your Safety”. CRC Press, 2010

manipulated (death is possible in less than one hour if the exposure is high), most Western Countries have deployed a set of detection systems and maintain communication networks in order to try to avoid their introduction and spread. However, these systems are mostly set-up at borders (roads, ports, airports and rail controls) and do not cover a large surveillance area but only zonal ‘pinch point’ sites. Moreover, they are highly sensitive, expensive, of large dimensions and not at all portable. It is therefore imperative to explore alternative and complementary detection strategies to the systems already in place.

Thus, as a complement of such limited, zonal systems, a breakthrough solution is proposed based on the implementation of much smaller detectors, able to detect both gamma radiation and neutrons, combined with GPS location systems and a wireless network. REWARD solution is a complete radiation monitoring system target to be installed to any form of mobile terrestrial transportation (car, bus, track, etc.) or can be installed in a network fashion across many fixed sites of a wide area. In this manner, REWARD is able to constantly monitor large, wide areas, hugely improving the needed surveillance of radiation sources whilst greatly incrementing the safety of the population at large.

REWARD aims to address the recommendations from the Final Report of the ESRIF CBRN Working Group[2] that underline: “Prevention is crucial and should receive particular attention by equipping intelligence agencies and policy makers with improved information analysis tools. Consequence management to overcome CBRN attacks and hoaxes requires networked warning and situational awareness systems with development of more effective and reliable detection and identification capabilities.” The re-port also quotes between the Research and Innovation Priorities: “Increased capacity (for Radiological/Nuclear incident preparedness) with small mobile detection devices.”

Security is today a key requirement for the conception of any information system and, depending on the particular application context, security concerns relate to the protection of systems against malicious attacks, the management of digital identity and trust, protection of data and privacy etc. On the other hand, security models consider different architectural levels such as network security (depending on the network infra-structure), operating system vs. application security (e.g. hacking an operating system or user application) and also the physical security (e.g. basic system access through passwords). Hence, the number of security issues and corresponding technologies is wide.

As regards the current framework of standards and good practices for Service-Oriented Architectures (SOA), one must consider the OASIS initiative[3] that promotes security standards (among others) needed in e-business and Web services applications. These standards range from common identity management to biometric identity assurance, policy management, digital signatures, privacy management, access control etc. to message protection cryptography.

For the REWARD ICT security, important design challenges stem from the fact that the solution architecture operates in a distributed, heterogeneous and wireless network environment. Therefore a

[2] ESRIF Final Report, December 2009
[3] https://www.oasis-open.org/

security framework was built and provided for the REWARD architecture, taking into account given reference architectures and implementations for Service-Oriented Architectures (SOA), which includes not only cloud deployments, but also addresses the particular operational security requirements derived from REWARD operational scenarios.

The main results of REWARD are highlighted in the following list:

- High efficiency radiation detectors, both for **gamma** radiation and for **neutrons**, have been developed using state-of-the-art technologies that offer superior performances, lower volume and lower cost compared to conventional sensors. The detectors have been optimized for detection efficiency and energy resolution.

- The integration of a gamma and a neutron detector unit in a single monitoring device, called **tag**. The combined information from both sensors makes easier to identify radioactive sources and nuclear materials, improving identification accuracy and reducing the occurrence of false identifications.

  REWARD tags are portable systems with small size and weight, target to be installed on vehicles. They are equipped with a positioning and communications unit (only used when no external resource is available) to communicate measurements to system upper layers. REWARD tags provides a radiation monitoring network that is capable of autonomous operation, is flexible and can easily be adapted to the needs and conditions of the specific situation. A specific application for instance, may not use one of the sensor systems so it can be removed, or may need the use of a different sensor type and the one in use now can be replaced. The system is be able to monitor large areas in real time and can be unobtrusively deployed even in places where large crowds are present.

- A **central monitoring and decision support system** have been developed with the ability to process the data from the sensing units (tags) and to compare them with historical radiation records. This provides improved detection capabilities even for low signal rates, increasing the reduction of the number of false alarms.

  A web application was developed to allow user interaction multi touch and multi user the outcomes were a natural approach to the application provided by the multi touch and a decision support in a collaborative and shared environment provided by multi user. These features are news if used inside a monitoring and control system.

  Another outcome for the CMS are the algorithms in particular the identification of the sources that is the first resolution step of a very complex problem that during the laboratory test has achieved very good results.

- A cloud based middleware package for the management and communication of the wireless sensor network with the central monitoring and decision support system. Providing scalable capabilities to handle from few sensor to thousands of them.

- A security framework to ensure protection against unauthorized access to the network and data, ensuring the privacy of the communications and contributing to the overall robustness and reliability of the REWARD system.

3 REWARD main S&T results/foregrounds

3.1 REWARD at a glance.

REWARD is a novel mobile system for real-time, wide-area radiation surveillance, based on the integration of new miniaturized solid-state radiation sensors. One sensor is a Cadmium-Zinc-Telluride (CdZnTe) detector for gamma radiation with precise energy measurement to identify the emitting isotope, integrating two sensors (19 x 19 x 5 mm) working in coincidence, a Coplanar Grid anode structure, FE Read Out Electronics (shielded) and a cooling system nearby[4]. The other detection subsystem is a neutron detector based on state-of-the-art sensing technologies that offers superior performances and lower mass and cost compared to conventional sensors. The sensors, optimized for slow neutrons, are based on novel silicon micro-machined structures for high detection efficiency filled with a lithium-based neutron converter. Several sensor boards are arranged around a polyethylene cube that is used to moderate the incident neutron spectrum. The detection of fast neutrons is done with ultrathin, low-background planar silicon sensors covered with hydrogenated plastic[5].

The nuclear radiation detectors form the core of a sensing unit (or tag) which includes the silicon-based neutron detector subsystem, the CdZnTe gamma detector system, a processor to control the whole unit performance and link the data to the communications equipment (self-supplied or car equipped one), the battery system and housing for the whole unit. A self-supplied wireless communication interface is also integrated to send the data remotely to a monitoring base station as well as a GPS system to calculate the position of the tag.

REWARD tags are small, mobile and portable modular units in the sense that virtually any number of sensing modules in a network is feasible, allowing the flexible adaption of the system to the end user needs. They can be deployed in patrol vehicles, emergency units and in general in any type of mobile equipment. The first prototype of REWARD sensing unit is shown in Figure 9.

REWARD’s tags targets easy integration and deployment in emergency systems at different levels, self-adapting to in-vehicle communication systems (TETRA, GPRS, etc…) embedded in modern law

[4] M. Dambacher, A.Fauler, C. Disch, A. Zwerger, J.P. Balbuena, U. Stöhlker, M. Fiederle, "Evaluation of Various Coplanar Grid (Cd,Zn)Te Detector Concepts for the Application in Gamma Radiation Surveillance and Environmental Monitoring Detection Systems", IEEE NSS/MIC/RTSD Conference, Seoul, 2013

[5] C. Guardiola, “Novel silicon sensors for neutron detection”, Thesis, Universitat Autonoma de Barcelona/CSIC, Spain

enforcement and civil protection vehicles. Tags upload geo referenced radiation information to a central server throughout REWARD's middleware. The TETRA communications network is used in REWARD project preferentially in order to ensure communication success even during overload situations, unlike the GSM/GPRS/3G options preferred by other networked sensor systems.

REWARD system (Figure 1) incorporates 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. Multiple sensing devices and the communication system are neatly coupled to a centralized processing module via a Sensor Abstraction Layer (SAL) component. Neutron and gamma count, collected by the sensors, are used to identify and to calculate the position of the radioactive source from the sensors' position, through algorithms based on geostatistical techniques[6]. The collected data are used to build a 2D map of the radiations in the area of interest. A security framework is also developed to ensure protection against unauthorized access to the network and data, ensuring the privacy of the communications and contributing to the overall robustness and reliability of the REWARD system.

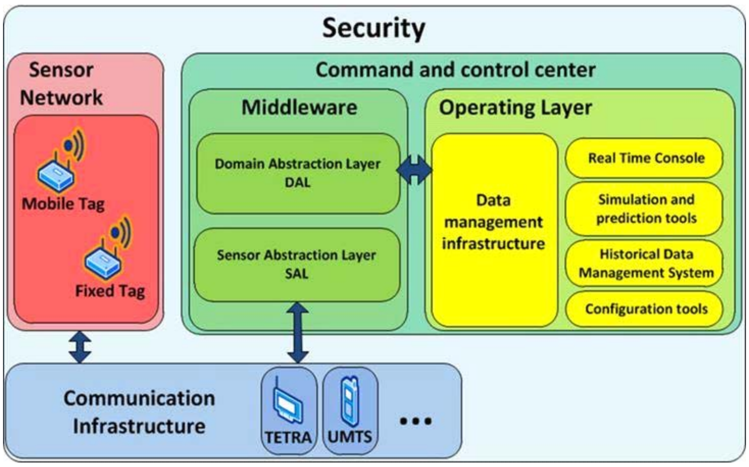

Security
Sensor Network
Mobile Tag
Fixed Tag
Command and control center
Middleware
Domain Abstraction Layer DAL
Sensor Abstraction Layer SAL
Operating Layer
Data management infrastructure
Real Time Console
Simulation and prediction tools
Historical Data Management System
Configuration tools
Communication Infrastructure
TETRA
UMTS
...

Figure 1: Reward system schema

REWARD's tag radiation, position and status information is sent to a Command and Control Centre. In order to communicate this information effectively, a middleware has been created to ensure the communication of information from/to the sensor tag to the high-level application (command and control center), and it is a tool for the management of the sensor network. REWARD's middleware provides necessary building blocks for easy integration within existing ICT infrastructure of the service provider (law enforcement or civil protection ICT infrastructures). The middleware operates in a heterogeneous and wireless network environment and enables communication and management of data in distributed applications. The main functions performed are; (*i*) Collect data, (*ii*) Analyse data, (*iii*) Data Aggregation/Data Fusion, (*iv*) Translate data, (*v*) Monitor Data, (*vi*) Transfer

[6] Heuvelink, Griffith, Space–Time Geostatistics for Geography: A Case Study of Radiation Monitoring Across Parts of Germany, Geographical Analysis n.42(2010), pp. 161–179

(Abstract Layer), (*vii*) Audit information, (*viii*) secure components and communications, (*ix*) Interoperability and Reliability.

Central Monitoring System (CMS) is part of the REWARD platform and its main functionalities are the data management, the data analysis and the data presentation. CMS receives live data, from the remote sensors network, through the middleware; it analyses and matches them with the radiation background of the surrounding area in order to create, in real time, geo-localized warnings when abnormal situations are detected.

The REWARD system is complemented with a horizontal component that takes care of the overall security of the system, called Security Framework. The purpose of this framework is mainly to ensure protection against unauthorized access to the network and data, ensuring privacy of communications and contributing to the overall robustness and reliability of the REWARD platform.

REWARD ICT solution architecture operates in a distributed, heterogeneous and wireless network environment. Therefore, the security framework was built and provided for this particular architecture. Apart from taking into account given security reference architectures and implementations for Service-Oriented Architectures (SOA), including Cloud deployments, the security framework also addresses the particular operational security requirements as derived from REWARD's operational scenarios.

Following this briefly introduction of REWARD, a more detailed explanation will be presented for its main components; (i) radiation sensor, (ii) tags, (iii) middleware, (iv) command and control centre and (v) security framework.

3.2 REWARD Scenarios

Before the design and development of REWARD started, an important work for REWARD was done, which consisted on the characterization of reference scenarios associated with RN threats, such as Radiological Dispersal Devices (RDD) and Improvised Nuclear Devices. Many Monte-Carlo simulations with state-of-the-art simulation codes were performed in order to study the radiation environment of these different scenarios. The most important parameters that define a radioactive security threat were studied: affected area, type and energy of radiation reaching the detector, effect of source type, shielding and distance on detectability. These simulations were particularized to the REWARD case and the response of the radiation sensors to these radiation scenarios was obtained in order to assess the required capabilities of REWARD's sensor system and subsequently test and validate them. Nevertheless, the results of the simulation work made for REWARD can easily be used to **identify the requirements that any other detection system aimed for homeland security should feature** in order to detect and identify the characteristic signatures of materials that can be potentially used in RDDs or other RN threats.

As an example, one of the scenarios considered a higher security risk is a Radiological Dispersal Device, commonly referred to as "dirty bomb". A RDD consists of radioactive material combined with conventional explosives, or even an aerosol[7]. These devices are designed to disperse radioactive material over a target area, contaminating individuals, equipment, facilities and the environment. The socio-economic consequences of the detonation of a RDD, namely the panic induced in the population and the costs and resources arising from the need to perform the radiological monitoring and eventual decontamination of considerable (urban) areas are often considered as largely exceeding the number of casualties that would arise from such event. To simulate the RDD, a source of 50.9TBq of ^{137}Cs, similar to the one involved in the radiological accident in Goiânia[8], was used as gamma emitter. Since most of the radioactive sources are sealed, a container was implemented, whose shielding material was varied, to evaluate the effect on the external gamma emission due to attenuation. The flux of particles reaching the detector was calculated at different distances from the center of the radioactive source. The results obtained revealed how the gamma fluxes are dependent on the characteristics of the radioactive source used as well as on the material and thickness of the shielding[9]. The non-radiological aspects of such devices fall outside the scope of this project and were not considered.

3.3 REWARD Radiation sensors

Detecting radioactive sources relies on measuring the gamma-rays or x-rays and/or neutrons emitted from the radioactive material. **REWARD has both neutron and gamma detection capabilities** unlike most of its competitors that usually detect only gammas. Neutron detection is key to detect the Pu or U in Improvised Nuclear Devices, and is a useful complement to gamma detection to help identify other sources with a neutron signature like 241AmBe. Thus, any radiation detection system used for homeland security should have both gamma and neutron capabilities. Common detection methods for gamma-rays and x-rays are frequently based on scintillation crystals, such as thallium activated sodium iodide (NaI(Tl) or often just NaI), which convert gamma radiation to light. Another detector technology is driven by solid-state semi-conductor detectors which convert the gamma-ray energy directly to an electronic pulse. Gamma detectors are mostly spectroscopic devices that measure the energy of the absorbed photon. Semiconductor detectors typically exhibit a significantly better energy resolution than scintillators, making them ideal for precise spectroscopy. In the REWARD project, a Cd,ZnTe semiconductor detector is used.

[7] C. Ferguson, T. Kaz and J. Perera, 2003. *Commercial Radioactive Sources: Surveying the Security Risks.* Occasional Paper Nº11. Center for Nonproliferation Studies.

[8] IAEA, 1988. *The radiological accident in Goiânia*. September 1988.

[9] M. Baptista, S. Barros, Y. Romanets, J. Marques, P. Vaz, C. Fleta, C. Jumilla, J. P. Balbuena, M. Dambacher, M. Lozano, U. Parzefall, 2013. *Monte Carlo simulations of radiological and nuclear terrorist threat scenarios: preliminary results of REWARD project*. 1st International Conference on Dosimetry and its Applications.

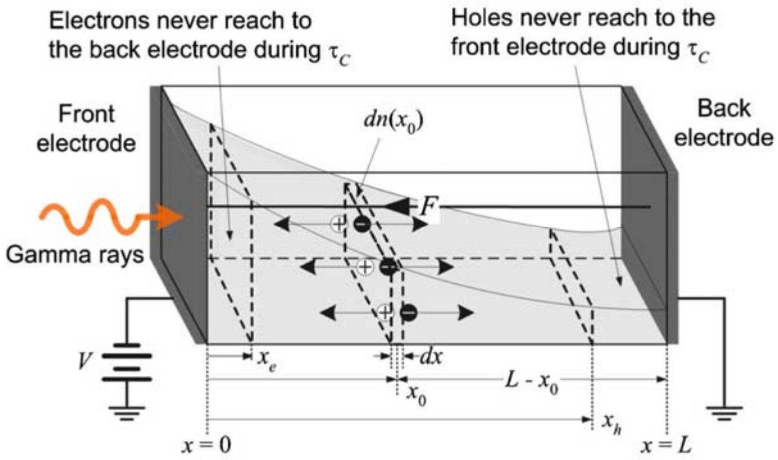

Electrons never reach to the back electrode during τ_C
Holes never reach to the front electrode during τ_C
Front electrode
$dn(x_0)$
Back electrode
F
Gamma rays
V
x_e
dx
$L - x_0$
x_0
x_h
$x = 0$
$x = L$

Figure 2: Schematic view of charge carrier transport and charge loss with carrier lifetime for electrons and holes in a planar semiconductor detector device.

The important advantage of the CdZnTe detector system is the possibility for energy resolving measurements. The CdZnTe is working like a miniaturized ionization chamber with the density of a solid state sensor. The emitted Gamma-radiation from a nuclear source is producing a cloud of positive and negative charge in the CdZnTe. The number of generated charged particles is proportional to the energy of the Gamma-radiation. In Figure 2 a sketch of the process of charge generation in a CdZnTe detector is shown.

The CdZnTe is the first choice of semiconductor detector materials regarding the energy resolution, operation at room temperature and availability

The contacts require a special design called Coplanar Grid CPG. This desgin allows an energy resolution better than 2 percent for a 662 keV Gamma-Ray photon. This feature enables the REWARD system to identify the radiation source by the isotope and validates the level of danger of a radioactive source. An image of the detector unit with the two CdZnTe detectors and the electronics is shown in Figure 3.

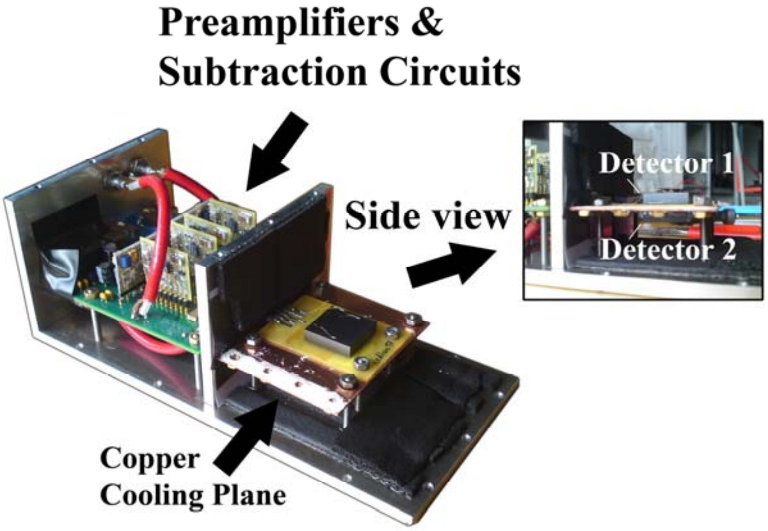


Figure 3: CPG (Cd,Zn)Te detector housing with two preamplifiers and one subtraction circuit per detector. A copper cooling plane between the two stacked detectors allows the application of temperature stabilization by connecting a Peltier cooler.

The complete Gamma Radiation detector unit is a very compact unit including the full electronics for the CdZnTe and a Multi Channel Analyzer GMCA. The GMCA is necessary to discriminate the energy of the radiation.

In Figure 4 a typical spectrum is given for the radiation source of ^{157}Cs with 662 keV. The shape of the spectrum and the peaks at different energy values are a fingerprint of the radiation source. These features will be used in the REWARD system for the isotope identification.

Neutrons do not interact with matter by ionization, thereby neutron detection methods in general rely on detecting the charged particles produced when neutrons react with a suitable material. Because REWARD's sensors are based on silicon, they are **compact, low-power, very stable with time, and unlike scintillators, are not affected by magnetic fields**. The signal produced by the interaction of a neutron is electronic making them ideal for portable systems which require integrated signal acquisition. The electronics to process the detector signals consists of analogue preamplifiers, pulse shapers and signal amplification. The counts in the different detectors are collected by a microcontroller, which can be read out by a PC or other computing device via a USB connector.

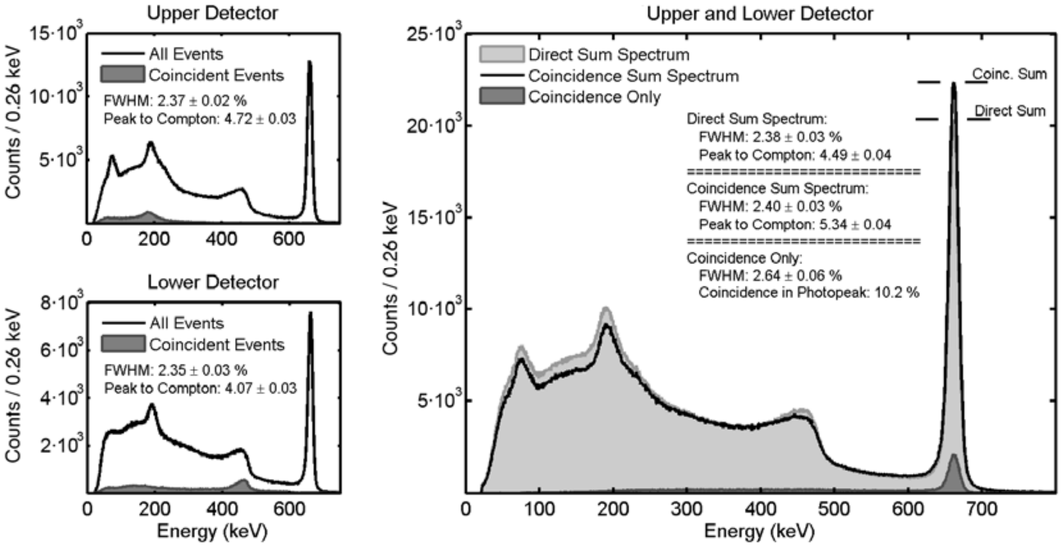


Figure 4: 662 keV 137Cs measurement with a stack of two CPG (Cd,Zn)Te detectors at a temperature of 10 °C. The graph shows the single detector spectra together with the comparison of the performance using the simple sum and the coincidence sum mode.

Two versions of silicon-based neutron sensors have been developed for the REWARD project: 1) ultra-thin sensors with extremely high gamma rejection ratio for demanding environments and 2) micromachined sensors with high thermal neutron detection efficiency.

3.3.1 Ultra-thin neutron sensors for high gamma rejection[10]

The detectors fabricated for the low-background version of the thermal neutron detector subsystem are thin-film diode charged particle sensors with a boron-based layer as neutron converter. Their lateral section is shown in Figure 5. The active silicon thickness of these devices is only 20 µm, which is enough to detect the signal from the neutrons but is **practically transparent to gamma photons**. This ability to distinguish between gamma and neutron radiation events is known as "gamma discrimination" and is of crucial importance for good neutron detectors as neutron radiation is typically accompanied by a gamma emission. The use of thin sensors has the added advantages of a good resistance to the adverse effects of radiation, a low operating voltage (5 V), low power consumption and insensitivity to voltage variations.

In order to detect thermal neutrons, a boron carbide converter layer was deposited on the front side of the detector. Boron carbide is one of the hardest materials known so it is a good option for applications in demanding physical environments. The entire detector fabrication process is **compatible with the processes of the microelectronic industry and can be used in large scale productions**.

[10] C. Fleta et al., 2014, *Fabrication and nuclear reactor tests of ultra-thin 3D silicon neutron detectors with a boron carbide converter*, Journal of Instrumentation 9 P04010, doi:10.1088/1748-0221/9/04/P04010

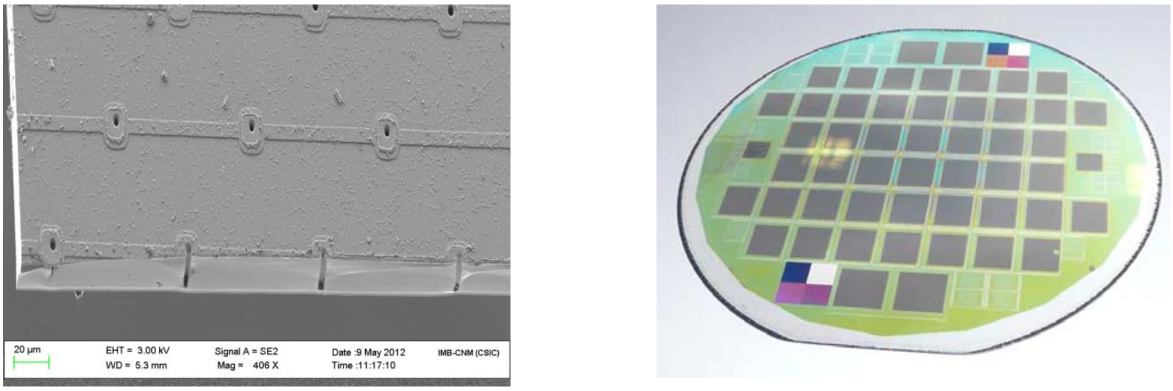


Figure 5: (Left) SEM cross-section of the ultra-thin silicon detectors. The active thickness is only 20 µm to ensure a high gamma rejection. (Right) Silicon wafer containing the neutron sensors.

3.3.2 Micromachined neutron sensors for high efficiency[11]

While the efficiency of typical planar neutron detectors is limited by the contact surface between the silicon and the converter, a perforated detector based on microstructures etched inside the silicon bulk can overcome this geometrical limitation and **considerably increase the neutron response**. In the new detectors specifically designed for REWARD, microstructures consisting of micro-channels filled with the neutron converter provide a high surface-volume contact ratio between the converter and the sensitive silicon bulk as can be seen in Figure 6.

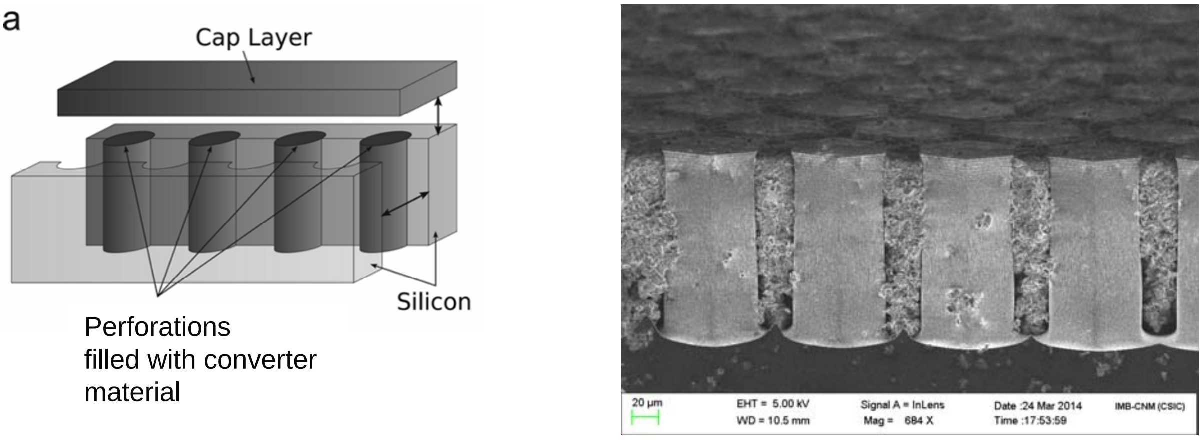


Figure 6: (Left) Structure of a perforated, high-efficiency neutron detector (Right) SEM image of the perforated structure filled with lithium-based converter.

The performance of REWARD’s detectors has been thoroughly tested with laboratory sources and with neutron beams at the Portuguese Research Reactor at IST/ITN. Both designs showed excellent performance as active neutron detectors. The ultra-thin detectors proved to be ideal for complex

[11] S. Esteban et al., 2014, *Microstructured silicon neutron detectors for security applications*, Journal of Instrumentation 9 C12006, doi: 10.1088/1748-0221/9/12/C12006.

mixed gamma–neutron radiation fields, which makes them useful for many applications besides security, such as **dosimetry in medical environments or in space**. The micromachined design increased the detection efficiency of typical silicon-based detectors by a factor of five, establishing the **next generation of neutron detectors for security applications**.

3.4 REWARD tag

REWARD system is based on **multiple independent units that form a mobile sensor network integrated with ICT technology already used** by the law enforcement and civil protection forces, like TETRA. These independent units, called **tags**, are a unique feature of REWARD and make it different from other systems.

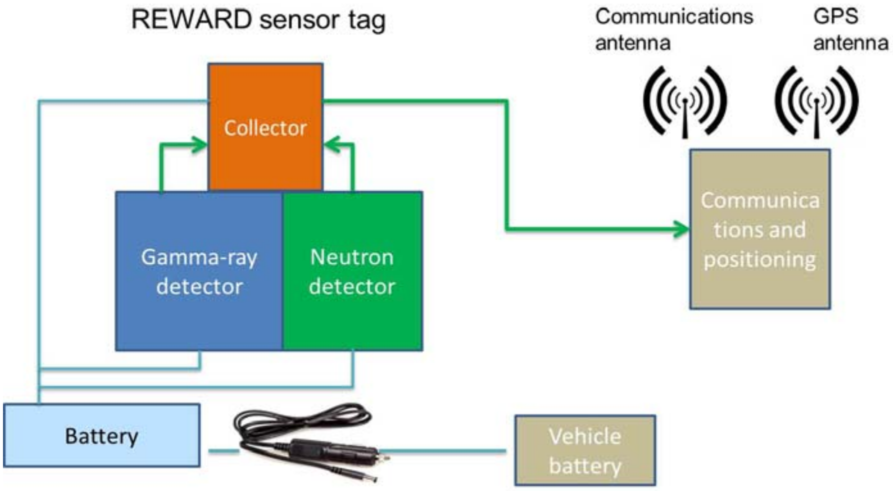


Figure 7: Components of the mobile sensor tag (Blue line indicates power, green indicates data line)

REWARD tags are the nodes of the network and consist on the integration of three subsystems into one single unit. The three subsystems in the tag are the neutron detector, the gamma detector and the communications subsystem. However, in order to control and make the communication possible among the different subsystem of the tag, another very important component is included in the sensor tag: the collector. This device is in control of the general behaviour of the sensor tag.

Figure 7 shows a logic overview of all the subsystems in the sensor tag and their connections. As can be seen, both sensor subsystems are connected to the central collector device. The collector device controls the timing of the measurements, receives the measurements from the sensors, keeps records of them, adapts the data to create a REWARD message and delivers this message to the communications system for its transmission over the wireless network.

The tag is the basic component of REWARD mobile network; therefore its development as a unit has been as important as the development of the individual radiation sensors. In fact, even though the tags are developed based on REWARD specific sensors and communication subsystems the integration has been done in a way that it is relatively simple to switch to a different sensor subsystem or communication equipment in case it is needed or better fits the needs of a particular application. These are other distinctive and important features of REWARD: its **adaptability and modularity**.

The design and integration of the different subsystems into one single unit has been done in three different aspects: logical, electrical and mechanical. All three of them have represented a considerable advance in the foreground of the project.

The logical integration refers to the communication among the different subsystems inside the tag. As mentioned before, one of the characteristics of REWARD is the easy integration with the systems already used by security forces. Due to this fact, special constrains have applied to the system. In order to ensure that the communications from REWARD would not be detrimental for other communications, the TETRA operators consulted advised in their use of the network. Based on this use, worst case scenario requirements were defined for the frequency and size of the messages sent by REWARD. This way REWARD is **adapted to work in very restrictive network conditions**, but is **also configurable for different transmission rates and message sizes**. These restrictions are handled by the central device that controls the general behaviour of the tag presented before. The collector not only manages the measurements cycles but it also collects the data from the different sensor subsystems. Both sensors use different ways of coding the information and the collector device needs to understand and process these data to construct the message to be sent. The data received from the gamma sensor is a complete spectrum; unfortunately, the transmission of a whole spectrum every 30 seconds (the acquisition time selected) could jam the radio channel, this is, it could overcharge the channel to the point of hindering other communications in TETRA. This may not be a problem in public networks such as the 3G mobile network but the data transmission is limited in others, such as the TETRA network. To reduce the volume of data sent a compression algorithm has been developed. This algorithm is part of the processing performed in the collector and represents another advance done throughout the project, since it reduces **a whole spectrum to a short text message and keeping an energy resolution better than 3% (at 662 keV)** at the same time.

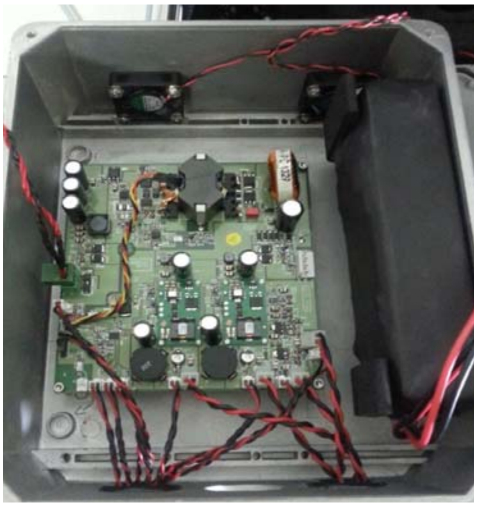


Figure 8: Battery system in its own housing.

The electrical integration of the REWARD tags has ensured that each particular power requirement each individual subsystem are met. The system has been designed to be powered up by the vehicle in which REWARD tag is carried. This way, the tag needs **no external battery**, only the standard power connection in the vehicle (+12V power plug). To improve the system even further, an additional battery is included in the tag. This battery ensures that the power supply is stable enough not to interfere with the readings or damage the electronics, plus it filters the noise from the car power line as well as cross noise among tag components. It also provides some autonomy from the vehicle power to the tag. This autonomy varies with the environmental conditions, especially temperature, but it is typically around 1 hour. This time is enough to make the tag independent of short stops of the engine, for instance to refuel, and even to be taken out of the vehicles while still working. The fact that the tag does not switch off when the vehicle engine stops for a short time **relieves it and the network from unnecessary tag initializations**. During operation, the battery system (see Figure 8) switches from a connected to a disconnected mode seamlessly to the rest of tag, therefore not affecting the normal functioning of the rest of the systems. That allows the tag to be moved from one vehicle to another without switching it off or even to be carried outside of the cars to take measurements as a handheld device. We conclude, as explained here, that the developed battery system offers great advantages: it makes the tag extremely **easy to install in a vehicle** since it only needs one connection to the standard power line, it **filters external as well as internal noise**, and it provides **autonomy to the tag**.

As for the electrical, the mechanical integration of the REWARD tags was carried out to comply with the needs of the individual systems while meeting the objectives for the overall tag. The encapsulation of the system should be robust enough to carry the electronics and protect them but it must not hinder the sensors reception of gamma and neutron radiation. After iterations in the design and fabrication, the encapsulation of the final prototype possesses several characteristics that make REWARD close to a finished product. A commercial housing has been used to reduce the price of the unit and ensures availability of supply. The design of the tag interior (components, support and cooling) allows the selection of housing similar to commercial systems with more limited features. The overall tag is **small and compact, and mobile and easy to transport**.

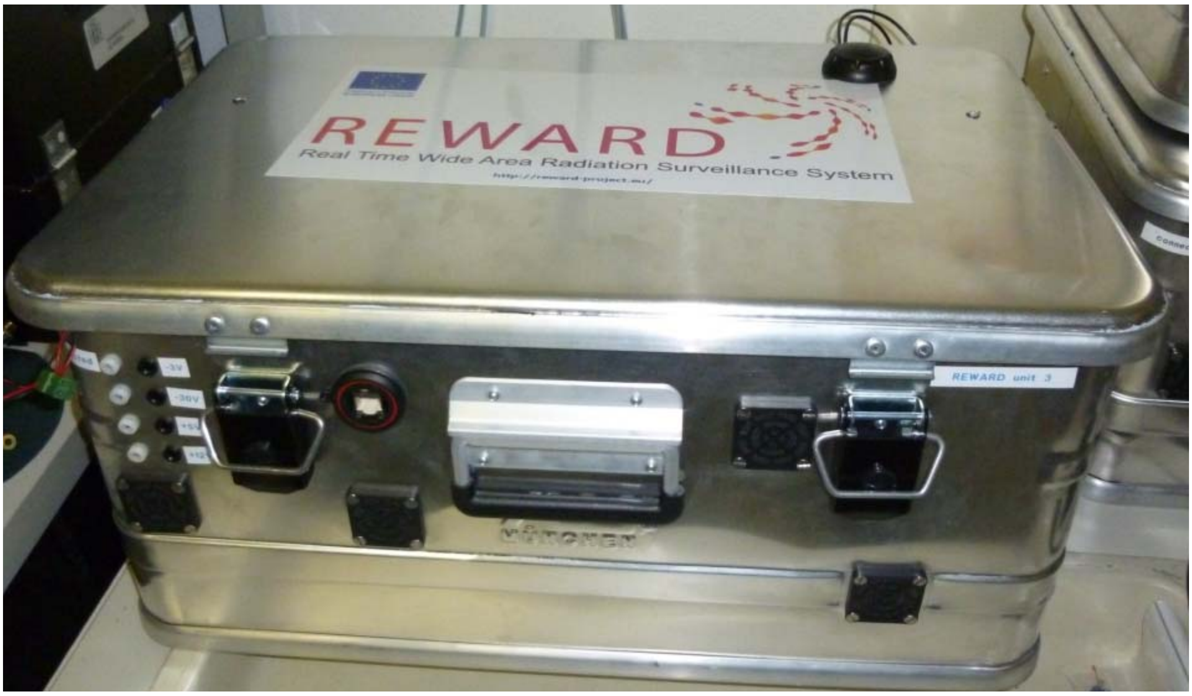

REWARD
Real Time Wide Area Radiation Surveillance System
http://reward-project.eu/
REWARD unit 3
-5V
-36V
+5V
+12
MÜNCHEN

Figure 9: REWARD tag

Furthermore, to ease the installation and the interaction with the equipment of the tag, there is only one connection to power it and one standard Ethernet connector to the collector inside. The RJ45 connector is used to connect the tag to the law enforcement or civil protection LAN infrastructure, it allows access to the collector via secure connection and allows the tag to send, to command and control centre, all buffered collected radiation measurement retained in it non-volatile memory. This feature is important in case the tag is used in data logger mode.

The tag’s communication subsystem handles the connection of tag with an in-vehicle communication system (like in case of TETRA equipped car, or internet connected car). When no external communication system is on the vehicle, the tag uses its own GRPS and GPS unit. By incorporating specific driver protocols, the tag will be able to connect to any particular equipment. Tag’s communication subsystem handles the communication lost with middleware (for instance, on low or loss of radio coverage) or with in-vehicle communication system. All radiation measurements are internally stored while radio communication is not available; an automatic upload is started as soon as radio communication is alive.

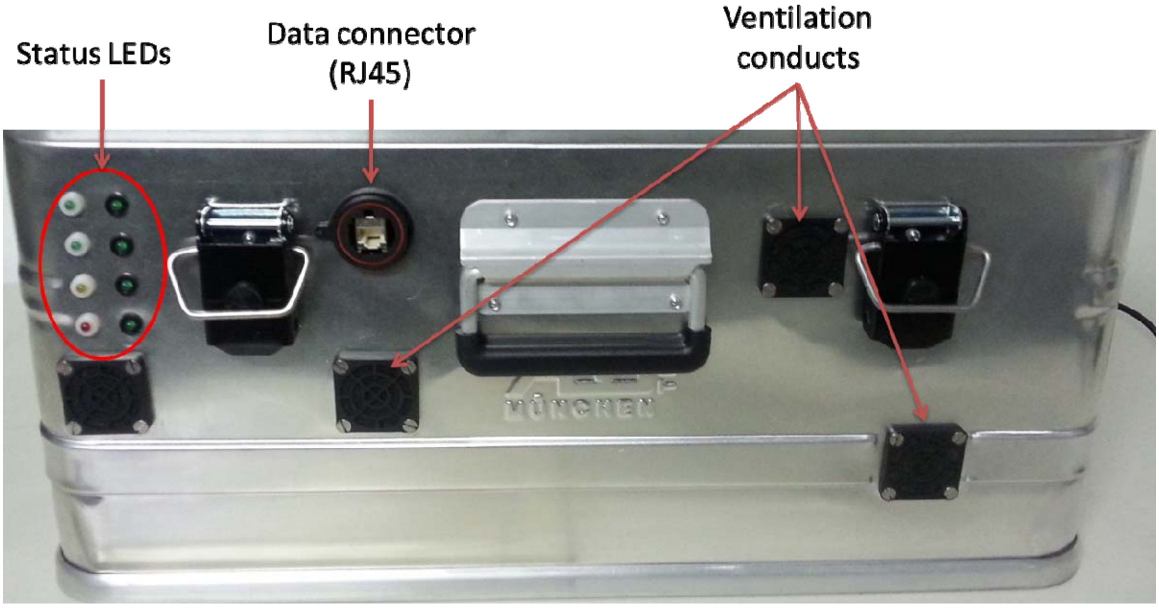


Figure 10: Detail of the tag housing.

In Figure 9 the data connector can be seen as well as some ventilation conducts and indication LEDs. The use of only one standard connection to communicate with the equipment inside improves the REWARD tag **usability** compare to other systems.

For flexibility, REWARD tag incorporates its own GPS and GPRS unit. This enables the use of the tag on any vehicle, even those without an in-car communication system. The communication connector uses standard serial interface as a way to connect with the in-car communication system. In case of a TETRA-equipped car, the tag is prepared to use car communication and GPS systems through the TETRA standard peripheral equipment interface. The tag can be customized to access other communication systems by incorporating specific protocols. In case of an internet connected car, the tag features plug and transmit capability.

3.5 REWARD Middleware

REWARD's middleware is a fundamental ICT piece that enables to connect seamlessly the real world (sensor network) with high-level applications, like the command and control centre software. It hides the complexity of wireless sensor network management and communication to the high-level application software, while delivering simplified status (of the network and sensors) and full rich real world measurements taken by the sensors deployed.

Middleware has been developed following a service-oriented architecture[12], and primarily target to be deployed on cloud infrastructures, but it allows on premises deployment for full customer flexibility. Thanks to its service oriented architecture and cloud deployment, the middleware is easily scalable, to provide service from few sensors to thousands of them. The software is laying on state of

[12] http://en.wikipedia.org/wiki/Service-oriented_architecture

the art cloud and software development technology, this form a good basis to become a reliable commercial software package from its prototype stage. Middleware components are designed with an N-Tier architecture approach. It is a model, suitable to support enterprise-level client/server applications by resolving issues like scalability, security, resiliency, fault tolerance, etc. Figure 11 shows the main building blocks. The Framework Foundations infrastructure works on two physical layers:

- Service layer. This includes business domains (user & app authentication, user & app registration, scheduling…). Everything is accessible to both local and remote clients.

- Client layer. Clients are connected to service layer over the wire, meaning that those can work with server infrastructure if they've LAN or internet connection. A client may be a Web site – Web-based products – or just a hardware sensor. Both end up using a REpresentational State Transfer (RESTful) Web Service Application Programming Interface (API).

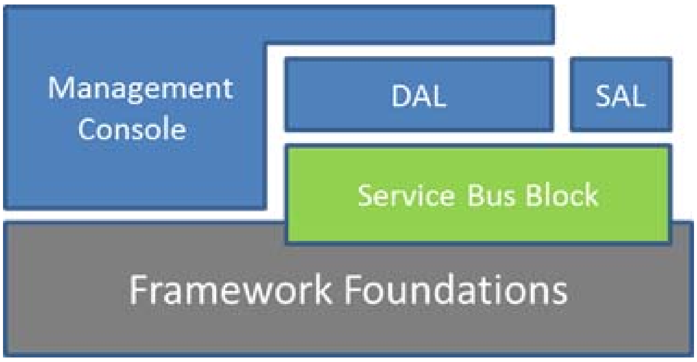


Figure 11: Middleware's main building blocks

The Service Bus Block is a group of software libraries, tools and user interface elements that provides default behaviours and visualization to queue monitoring. It provides sensor activity queuing and subscription system. It implements functionalities to manage the service oriented architecture. Its main goal is no other than easing the communication of sensors and its monitoring, and it exposes a RESTful open API using industry standards. Besides, Service Bus Block provides out-of-the-box reporting and user interface components for data visualization which makes life easier reporting on-screen activity and allowing interaction with sensor networks. Here is a quick feature list of inherited capabilities:

- Fully-stateless, token-based application and user authentication and authorization.
- Object-relational mapped (OR/M) data store, primarily using Entity Framework Code First which maps domain model to Structured Query Language (SQL) Server Azure and/or SQL Server 2012.
- Managed hashing and Advanced Encryption Standard (AES) encryption.
- Application & User registration and management.
- Common user interface elements.
- JavaScript client framework and RESTful programming toolkit.

DAL is the acronym of Domain Abstraction Layer and is responsible to interconnect the middleware to third party tools that enables decision support systems like the Central Monitoring System (CMS). One of the key aspects of the middleware is to be interoperable and open to be used by other software components that enable the creation of an ecosystem. DAL provides an API and endpoint to get information about the middleware and tags. Service oriented architectures are providing mechanisms to publish/subscribe messages. All the components connected to the middleware are able to receive the data coming in real time and transparently. This way DAL abstracts the Domain model (or so called it: the business) to the other components. The main function of the DAL is, once the tag messages are received (and transformed into eXtensible Markup Language (XML), like in the case of TETRA) they are processed on subsequent packages in the DAL sub-system. Afterwards, they are made available for subscription to upper layer software components like the Central Monitoring System. It is responsible as well to manage the acknowledgement flow of information between components.

SAL is the acronym of Sensor Abstraction Layer and is responsible of connecting devices (tag) to the upper layer of the REWARD middleware, the DAL. There is a need to abstract the underlying implementation of the wireless sensor network to the components involved in the project. SAL will connect and manage all the information from the sensors and adapt it to be consumed by upper layers. Some of the functionalities that are related to the SAL are:

- Parsing raw data from the sensors
- Adapt sensor data to human-computer readable format to be interchanged
- Manage sensor status
- Manage communications between components
- Data aggregation/Data fusion
- Manage command actions to be performed on tags
- Secure communications
- Abstract networks (TETRA, GPRS, ...)

Both blocks (SAL and DAL) have been architected to allow deployment flexibility in different devices and complex ICT infrastructures. For instance, SAL is capable to handle communication through TETRA and public IP infrastructures (GPRS, 3G, 4G…), depending on the selection (i.e. customer requirements), specific modules will be enabled at different REWARD components and customer ICT infrastructures. In case of TETRA, specific SAL driver runs on customer premises as it is tied to TETRA a specific radio receiver, while in case of public IP network, the SAL driver runs directly integrated within REWARD’s tag connecting them directly to DAL building block services. This feature can be further exploited by enabling real time selection of the communication infrastructure offered by the in-car communication system[13], the selection can be implement at REWARD’s tag, and it depends on the customer policy for the creation communication rules.

[13] As it is explain in the public REWARD project deliverable D1.6, it is common to find multiple communication channels in modern vehicles from security and civil protection forces.

SAL components inherits its flexible deployment capabilities by the selected development technology and the main hardware controller of REWARD's tag. It is developed in JAVA, thus it is almost practically universally portable to modern platforms similar to Raspberry Pi[14] and/or JAVA enabled platforms.

The communication between middleware's SAL and REWARD's tag is bidirectional. This allows modifying tag behaviour depending on command and control centre decisions (taking either by decision support system or operator). The most typical decisions would be the selection of tag message type to be sent or disable temporarily sending messages depending on the available communication network bandwidth. Decision at this level fully depend on the law enforcement or civil protection forces actuation protocols, it is important to state that the integration of actuation protocols were not the scope of REWARD project.

Data fusion and data aggregation capabilities is another important feature on middleware. Although this capabilities can be exploited at SAL and DAL level, are more relevant at DAL. REWARD components, specially the ICT building blocks, have been designed to reduce the integration time within customer ICT infrastructure and use available information. Let's take in-vehicle positioning system as an example, modern law enforcement and civil protection forces vehicles (and TETRA enabled ones) are equipped with a positioning system, which provides related GPS data used at the command and control centre to manage human and vehicle resources at a given time. Thus, GPS information is already being send and stored on specific databases at law enforcement and civil protection ICT infrastructures. Communication bandwidth is a gold treasure in case of emergency event, it must be used responsibly by humans and machines, specific rules and actions are taking from the command and control centre to maintain communication bandwidth for what it matters at all emergency event period. Under this real case, REWARD's tag must not sent its own GPS information (as it is a waste of communication bandwidth). Meaning that DAL is responsible to acquire GPS data from the law enforcement or civil protection databases and aggregate it to the message delivered to the command and control centre software. The integration with current ICT infrastructure at civil or law enforcement forces is enabled by accessing exposed RESTful services[15] (or similar SOAP/WSDL[16]), but when they are not available only specific drivers would need to be developed to access external databases.

The data flow between REWARD tags and command and control centre is performed by queues managed by DAL component, and it includes middleware inner communication. All publishers and subscriber tiers follows an authentication and authorisation DAL's procedure prior to access to the queue resources, data between tiers flows on encrypted communication channels. The security framework is integrated with the middleware components, prescribing horizontal features and integrating ad-hoc features such as tags white/black lists (further explanation about security framework is given later within this section). Queues are created/deleted automatically by DAL component upon request from authorised tags. One queue per tag is created to increase

[14] http://www.raspberrypi.org/
[15] http://en.wikipedia.org/wiki/Representational_state_transfer
[16] http://en.wikipedia.org/wiki/Web_Services_Description_Language

communication robustness and resilience. DAL's controller component monitors all queues and provide timely report events to an event manager, which is responsible for the communication of status messages, from queues, tags and statistics calculated in real time by DAL to subscribed clients.

All REWARD's visualisation features related with information captured by tags are provided by REWARD's command and control centre software. The middleware provides a simplified graphical user interface called Management console, it is responsible to show the correct functioning of the middleware and its components. The default client and user interface platform is a Web browser. This way, an administrator is able to know on real time and anywhere the status of the system regarding REWARD's middleware. Management console is a web client of Service Bus Block based on DAL features and API covering these functional areas:

- User authentication.
- User registration.
- Queuing management.
- Reporting and stats visualization (including tag measurement in raw format).

The client implements such features as visual components consuming data from DAL RESTful API over HyperText Transfer Protocol over Secure Socket Layer (HTTPS).

The goal of the management console and the API is twofold, on one side provides complementary channel to access tags measurement in real time besides the command and control centre software, this capability has been a helpful during integration and testing phase in the project. This tool then it can be used for the integration of the middleware into 3rd party tools & systems, as a testing tool and/or use the source code as starting building block for the development of new specific functions for a given client (even developed by the potential client itself). This feature highlights again one of the goals of the middleware, ease the integration phase of REWARD technology into the client (law enforcement and civil protection forces) ICT infrastructure. The other goal was to provide a mechanism for the control of the communication between the tags and the middleware, as a way to exploit the bidirectional communication between middleware and tags.

3.6 REWARD Decision support system

REWARD's Central Monitoring System (CMS) is part of the REWARD platform and its main functionalities are the data management, the data analysis and the data presentation. CMS has in charge to receive live data, from the remote sensors network, through the middleware; these data are analysed and is performed a matching with the radiation background of the surrounding area in order to detect, in real time, geo-localized warnings when abnormal situations are detected.

CMS provides to the operator the interfaces needed to perform the monitoring of the area and the analysis of the measures gathered by the mobile sensors. The main functionalities of CMS are:

- To support the decisions when threat situations are detected. CMS provides a set of tools to analyse, not only real-time data, but also the historical data in order to correlate all these information and to help the operators in their decisions.

- To process in real-time mode the received data. CMS elaborates the information by means of the data analysis algorithms.

- To provide the simulation tools. It is able to generate various scenario using a simulation methodology based on interacting agents, which, taking into account a variety of complex phenomena at the same time the operator can monitor the evolution of the simulated scenario using the instruments provided by the console as if it was in a real environment.

- To provide an architecture for the dissemination of signals/messages.

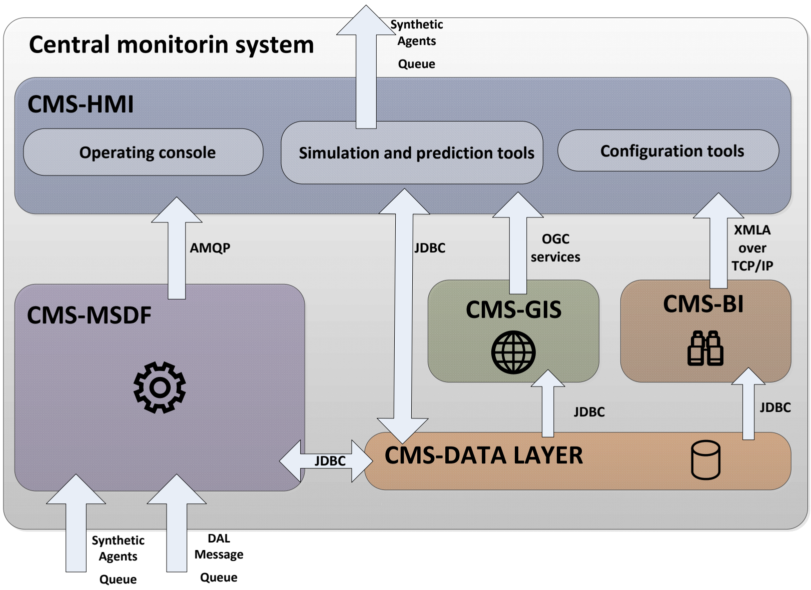


Figure 12: Central Monitoring System's main building blocks

CMS is composed by the several elements (see Figure 12), the main of them will be described below.

CMS-DATA LAYER: has in charge the persistence of the data. That is achieved by means of a **Database Management System (DBMSs) and file system**. Into CMS-DATA LAYER, from a logical point of view, different storages are identifiable: data storage, spatial storage, configuration storage and gamma spectrum reference storage. The data storage contains all the measurements received and the alarms detected by CMS. Into the spatial storage are saved the information used by the GIS infrastructure (maps, vector data…). The configuration storage contains the information related to the configuration of CMS. Finally, the gamma spectrum reference storage contains the dataset of sample gamma spectrums used from the identification algorithm.

CMS-MSDF: is the Multi-Sensor Data Fusion element, the core element of CMS; it provides to the central monitoring system the capabilities of multi sensor data fusion. The low level of CMS-MSDF is occupied by the Sensor Middleware subcomponent. This is used to subscribe to the DAL Message Queue and to gather the messages provided by the sensor network. CMS-MSDF allows extending its functionalities by adding pluggable data computation (plug-in technology) as Virtual Sensor.

Virtual Sensors in CMS-MSDF execute the algorithms for analysing of the radiation data collected by sensors. The data analysis algorithms are mainly based on the gamma spectrum, which has the characteristic features shown in Figure 13 .

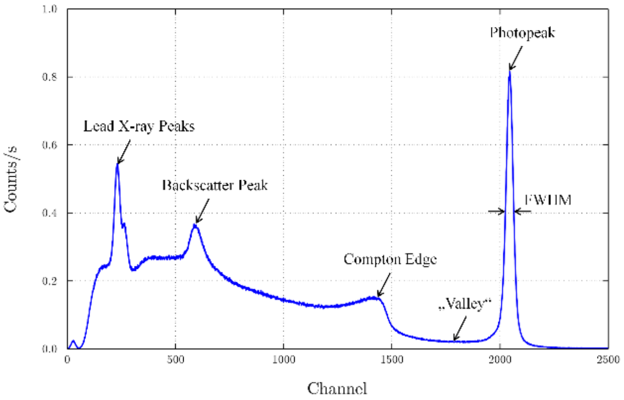


Figure 13: Example gamma spectrum features

To **identify a radiation source**, the most important piece of information is the position and number of photopeaks, due to photoelectric interactions in the detector. A gamma source can be identified by comparing the peaks in the incoming spectrum with the known data in a reference database of radionuclides. Other defining characteristics, such as the Compton edge, can also provide important information.

A function that interpolates various points of observations in the space is a central part of the decision support system, furthermore it estimates the level of radiation even in the point in which no measurements were collected. This calculation depends geolocalization of the measurements and its value, which in the case of the REWARD system is the count per second (cps) of the gamma spectrum. The algorithm used to interpolate the points is the Inverse Distance Weighted (IDW) which follows the non-statistical approach, because cps haven't got a direct relationship with the geographical position of the measurement. This conclusion was made after a huge stage of analysis with other algorithms to decide which was the best algorithm to follow.

The results of the interpolation function is used to construct a **radiation map** which represent different levels of radiation with different colours (colours and the scale are configurable) and points out graphically where the treat is localised. The algorithm that allows the system to estimate the geographical position of the (potential) source of dangerous radiations, is based on the radiation map and it is an adaptation of the Connected Component Label Algorithm (CCL). It classifies the various points of the radiation map as dangerous or not, simply comparing them with a configurable threshold. After this step, a threshold image is obtained. On this image the CCL Algorithm is applied in order to have aggregated zones with connected “dangerous” points of measurements. The estimation of the position of the source is computed simply by finding the centroid of the single aggregated dangerous zone.

An **identification algorithm** has been developed that allows the system to recognize the isotope which is responsible of the dangerous radiations. This result is obtained comparing the incoming spectrum and analyse its photo peaks. Before this step, an elaboration of the spectrum is needed to remove the background noise. Once computed the elaborated spectrum, it is compared with Gaussian approximation of the known spectrum of the various radioactive isotopes (i.e. Ra-226, Am-241, Cs-137, Co-60 etc.). If the similarity (computed as the covariance between the two spectra) is high, that radiation was recognized as that isotope. This algorithm runs only if the cps of the measurement exceeds a threshold.

CMS-GIS is the Geographic Information System (see Figure 14). The aim of CMS-GIS component is to make available the capabilities of management and presentation of spatial data. Additionally, to achieve these purposes, it has to use a standardized interface. In order to provide such functionalities, the component implements the Open Geospatial Consortium (OGC) standards, i.e. Web Map Service (WMS) for operations on maps and Web Feature Service (WFS) for operations on features.

The architecture developed for CMS-GIS component allow to manage not only 2D spatial data, but also 3D.

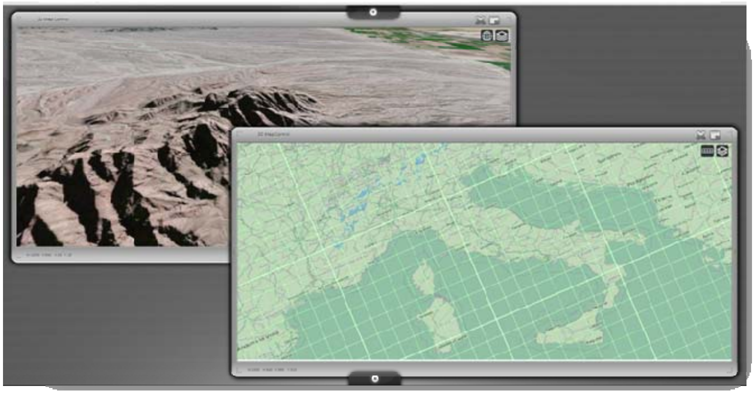


Figure 14: CMS-GIS user interface

CMS-BI represents the Business Intelligence component of the central monitoring system. The goal of CMS-BI is to enhance the decision-making features of CMS. CMS-BI component includes two subcomponents: Data warehouse and Business Intelligence. CMS-BI implements the business intelligence architectural stack, which refers to data preparation and data usage as two separate, but closely linked segments of the same architecture. CMS-BI performs the analysis of historical data of the measurements to the area of interest is achieved by adopting a business intelligence solution based on Microsoft SQL Server OLAP Services: SQL Server Analytical Services.

The prospects considered useful for observing these quantities are:

- The geographical dimension.
- The dimension of time to be organized by year, month, day of month, day of week, time.
- The size of material of the radioactive source.

The technologies adopted by CMS-BI provide historical views of operations. Furthermore, it provides functionalities of **reporting and data mining** (i.e. data analysis over time and space).

CMS-HMI is the **Human-Machine Interface** (see Figure 15) and it aims to provide the user interface of the central monitoring system. It provides to the operator the tools to interact with the system, in order to execute the ordinary and extraordinary surveillance activities.

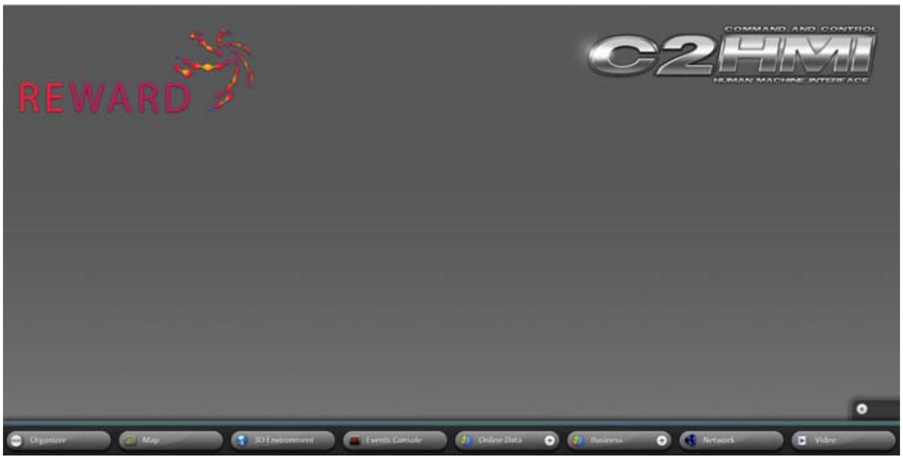


Figure 15 - CMS-HMI

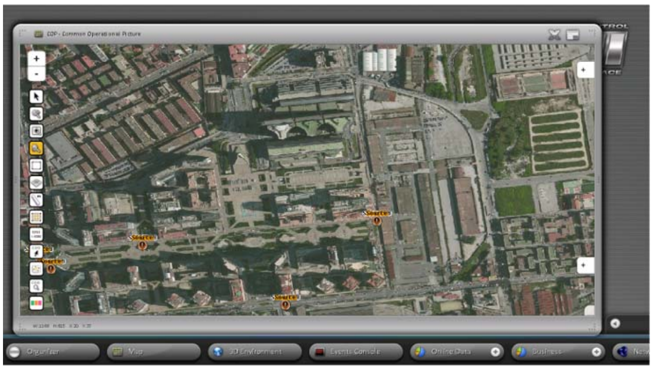
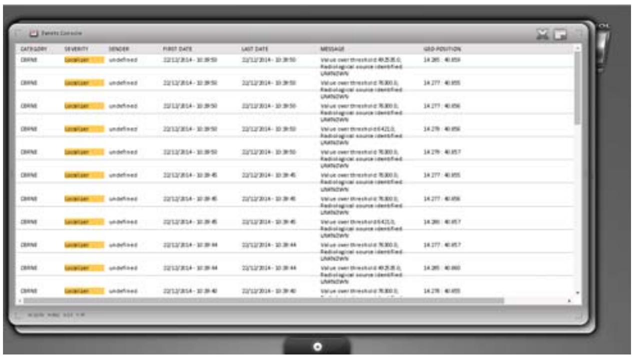


Figure 16: CMS-HMI - 2D map control


Events Console

CATEGORY	SEVERITY	SENDER	FIRST DATE	LAST DATE	MESSAGE	GEO POSITION
CBRNE	Localizer	undefined	22/12/2014 - 10:39:50	22/12/2014 - 10:39:50	Value over threshold 49253.0, Radiological source identified UNKNOWN	14.285 : 40.859
CBRNE	Localizer	undefined	22/12/2014 - 10:39:50	22/12/2014 - 10:39:50	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.277 : 40.855
CBRNE	Localizer	undefined	22/12/2014 - 10:39:50	22/12/2014 - 10:39:50	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.277 : 40.856
CBRNE	Localizer	undefined	22/12/2014 - 10:39:50	22/12/2014 - 10:39:50	Value over threshold 6421.0, Radiological source identified UNKNOWN	14.279 : 40.856
CBRNE	Localizer	undefined	22/12/2014 - 10:39:50	22/12/2014 - 10:39:50	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.279 : 40.857
CBRNE	Localizer	undefined	22/12/2014 - 10:39:45	22/12/2014 - 10:39:45	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.277 : 40.855
CBRNE	Localizer	undefined	22/12/2014 - 10:39:45	22/12/2014 - 10:39:45	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.277 : 40.856
CBRNE	Localizer	undefined	22/12/2014 - 10:39:45	22/12/2014 - 10:39:45	Value over threshold 6421.0, Radiological source identified UNKNOWN	14.280 : 40.857
CBRNE	Localizer	undefined	22/12/2014 - 10:39:44	22/12/2014 - 10:39:44	Value over threshold 76300.0, Radiological source identified UNKNOWN	14.277 : 40.857
CBRNE	Localizer	undefined	22/12/2014 - 10:39:44	22/12/2014 - 10:39:44	Value over threshold 49253.0, Radiological source identified UNKNOWN	14.285 : 40.860
CBRNE	Localizer	undefined	22/12/2014 - 10:39:40	22/12/2014 - 10:39:40	Value over threshold 76300.0,	14.278 : 40.855

Figure 17: CMS-HMI - Alarm panel

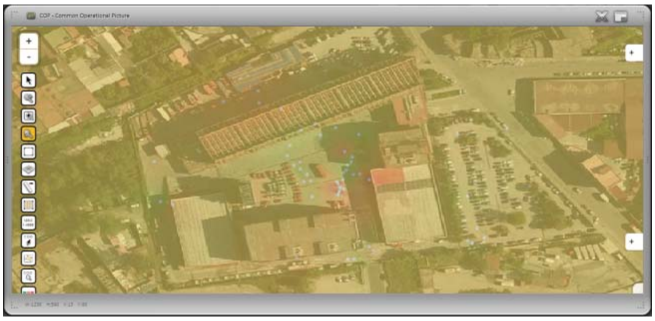
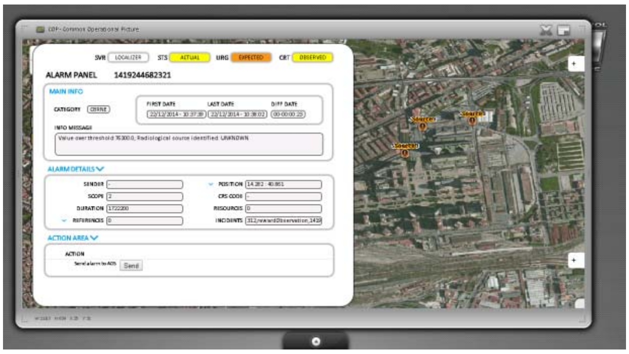


Figure 18: CMS-HMI - Radiation map



SVR LOCALIZER STS ACTUAL URG EXPECTED CRT OBSERVED

ALARM PANEL 1419244682321

MAIN INFO

CATEGORY: CBRNE

FIRST DATE: 22/12/2014 - 10:37:39
LAST DATE: 22/12/2014 - 10:38:02
DIFF DATE: 00:00:00:23

INFO MESSAGE: Value over threshold 76300.0; Radiological source identified: UNKNOWN

ALARM DETAILS

SENDER: -
SCOPE: 2
DURATION: 1722200
REFERENCES: 0
POSITION: 14.282 : 40.851
CRS CODE: -
RESOURCES: 0
INCIDENTS: 312/rewardObservation_1419

ACTION AREA

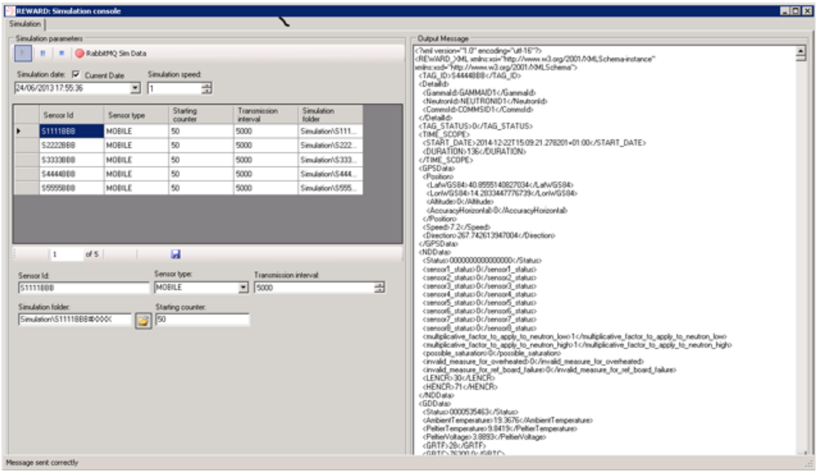
ACTION
Send alarm to AOS

Figure 19: CMS-HMI – CAP alarm detail panel

The **Operating console** represents the core component of CMS-HMI. It is the real user interface of Central Monitoring System and the operator can access to all its features through the operating console. Different views representing the **common operational picture** (COP) are represented in Figure 16 to Figure 19. The operating console implements an innovative interaction paradigm based on multi-touch and multi-user features.

The decision support system provides also a **simulation and prediction tool** component. This component allow user to define and to activate the simulation environment (Figure 20 provides and snapshot of the tool). The developed simulation, is able to generate various scenario using a simulation methodology based on interacting agents which, taking into account a variety of complex phenomena. Simulator software is also capable to taking into account of a variety of different types related to radioactive sources.

The operator will have an interface through which he can set up a simulation choosing sensors number, their position, the path, the source position and source type. When the simulator is on, it can read measures file that are precomputed by Monte Carlo Simulation or by a true measurement campaign, and it can reproduce the chosen scenario, in this way the operator can monitor the evolution of the simulated scenario using the instruments provided by the console as if it was in a real environment. Using the same instruments of the real activities, users can be trained.



Simulation date: ☑ Current Date
24/06/2013 17:55:36

Simulation speed: 1

	Sensor Id	Sensor type	Starting counter	Transmission interval	Simulation folder
▶	S1111BBB	MOBILE	50	5000	Simulation\S111...
	S2222BBB	MOBILE	50	5000	Simulation\S222...
	S3333BBB	MOBILE	50	5000	Simulation\S333...
	S4444BBB	MOBILE	50	5000	Simulation\S444...
	S5555BBB	MOBILE	50	5000	Simulation\S555...

1 of 5

Sensor Id: S1111BBB

Sensor type: MOBILE

Transmission interval: 5000

Simulation folder: Simulation\S1111BBB#XXXX

Starting counter: 50

```
<?xml version="1.0" encoding="utf-16"?>
<REWARD_XML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <TAG_ID>S4444BBB</TAG_ID>
 <DetailId>
  <GammaId>GAMMAID1</GammaId>
  <NeutronId>NEUTRONID1</NeutronId>
  <CommId>COMMSID1</CommId>
 </DetailId>
 <TAG_STATUS>0</TAG_STATUS>
 <TIME_SCOPE>
  <START_DATE>2014-12-22T15:09:21.278201+01:00</START_DATE>
  <DURATION>136</DURATION>
 </TIME_SCOPE>
 <GPSData>
  <Position>
   <LatWGS84>40.8555140827034</LatWGS84>
   <LonWGS84>14.2833447776739</LonWGS84>
   <Altitude>0</Altitude>
   <AccuracyHorizontal>0</AccuracyHorizontal>
  </Position>
  <Speed>7.2</Speed>
  <Direction>267.742613947004</Direction>
 </GPSData>
 <NDData>
  <Status>0000000000000000</Status>
  <sensor1_status>0</sensor1_status>
  <sensor2_status>0</sensor2_status>
  <sensor3_status>0</sensor3_status>
  <sensor4_status>0</sensor4_status>
  <sensor5_status>0</sensor5_status>
  <sensor6_status>0</sensor6_status>
  <sensor7_status>0</sensor7_status>
  <sensor8_status>0</sensor8_status>
  <multiplicative_factor_to_apply_to_neutron_low>1</multiplicative_factor_to_apply_to_neutron_low>
  <multiplicative_factor_to_apply_to_neutron_high>1</multiplicative_factor_to_apply_to_neutron_high>
  <possible_saturation>0</possible_saturation>
  <invalid_measure_for_overheated>0</invalid_measure_for_overheated>
  <invalid_measure_for_ref_board_failure>0</invalid_measure_for_ref_board_failure>
  <LENCR>30</LENCR>
  <HENCR>71</HENCR>
 </NDData>
 <GDData>
  <Status>0000535463</Status>
  <AmbientTemperature>19.3676</AmbientTemperature>
  <PeltierTemperature>9.8419</PeltierTemperature>
  <PeltierVoltage>3.8893</PeltierVoltage>
  <GRTF>28</GRTF>
  <GRTC>76300.0</GRTC>
```

Message sent correctly

Figure 20: CMS-Simulation Console

CMS-HMI, following a natural user interface paradigm[17], it allows to the operator being able to quickly transition from novice to expert. The main design principles followed during the development are:

1. ***Easier deployment, scalability and easier maintainability***: The use of the latest web standards and technologies allows to have a platform-independent software system which is:

    a. ***simple to deploy***: the platform has to be deployed on a single machine and is automatically accessible to all the devices with a network connection;
    b. ***simple to maintain***: updates have to be delivered to a single machine;

2. ***Multi-user, touch environment***: CMS-HMI exploits the potential benefits given by the use of multi touch tablets. The elements of the console react to touch inputs.

3. ***Extensible widgets***: CMS-HMI is made up by reusable modules called widgets.

4. ***Standard communication protocols***: CMS-HMI communicates using standard communication protocols and specifications. Specifically, protocols like WebSocket, Server-Sent Events and HTTP are used. Geospatial data is delivered through the main protocols defined by the Open Geospatial Consortium (OGC): Web Feature Service (WFS), Web Coverage Service (WCS) and Web Map Service (WMS) protocols.

5. ***Open source stack:*** CMS-HMI integrates the most commonly used, open source, third party libraries and encapsulates them into self-contained components. jQuery library, a small and fast Javascript library, is used to simplify web document manipulation. The web pages are served through an instance of the Apache HTTP Server. Furthermore, geospatial data is served using GeoServer, which implements the OGC standards and the INSPIRE European directive. The OpenLayers library is used to visualise bidimensional cartography while the

[17] http://research.microsoft.com/en-us/collaboration/focus/nui/

CesiumJS is used for data visualisation in a three- dimensional representation of the region of interest.

Finally, CMS is equipped with a **dissemination infrastructure**, which allows the operator to send signals/messages to other systems or stakeholder when abnormal situations are detected. The system is based on a specific architecture, which allows the diffusion of appropriate alarms (and /or warnings) to particular categories of people. This system also allows the setting of some configuration parameters (such as email addresses and RSS) in order to allow the dissemination of alarms to a wide audience of persons that have different roles and abilities. The dissemination of signals/messages are performed using a standard protocol called Common Alerting Protocol (CAP[18]).

3.7 REWARD Security Framework

Concerning the ICT security objectives, stated in the section above, considered by the consortium, in order to secure the REWARD SOA system architecture, lead to the design and construction of a dynamic and reusable security framework – the REWARD Security Framework.

This REWARD Security Framework is generically described by as:

- a well-documented set of security and configuration best practices; leveraged by
- a set of identified & selected security software packages (Horizontal Security); and
- a set of specific developed secured software components (Ad-Hoc Security).

The **main objective** of this framework is to secure the REWARD distributed system (SOA) and its communication interfaces.

Among the existing security paradigms and having in mind the REWARD system objectives, an extended version of the CIA[19] security concept was selected and applied. Please note the diagram depicted in the figure below.

[18] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html

[19] Confidentiality, Integrity, and Availability

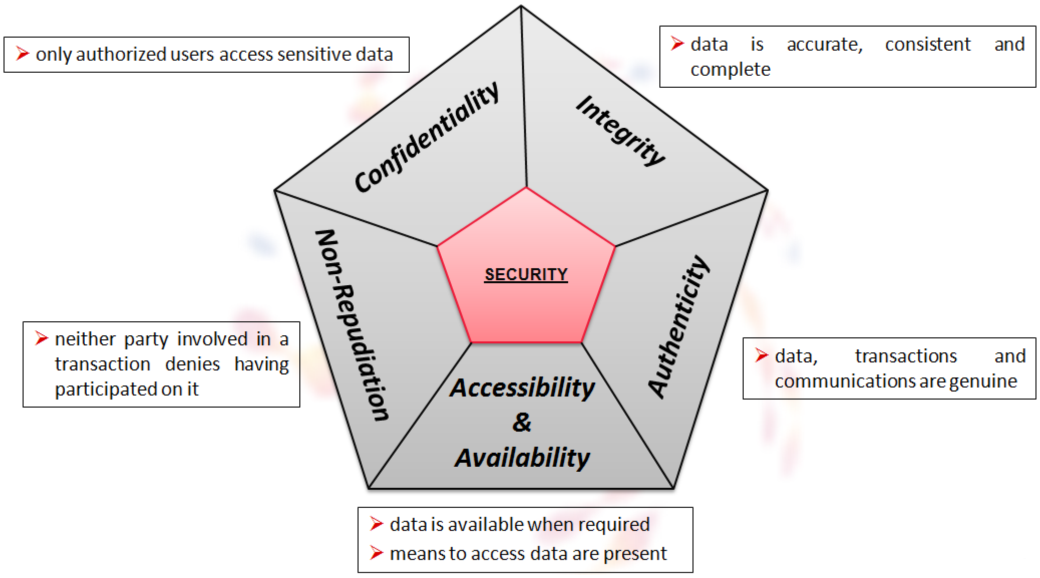

only authorized users access sensitive data
data is accurate, consistent and complete
Confidentiality
Integrity
SECURITY
Non-Repudiation
Authenticity
Accessibility & Availability
neither party involved in a transaction denies having participated on it
data, transactions and communications are genuine
data is available when required
means to access data are present

Figure 21: REWARD ICT Security Concepts & Principles

The Security Concepts and Principles approach (represented in Figure 21), elected for the REWARD system, can be generally summarized as follows:

- Confidentiality - Ensuring only authorized users' access sensitive data.
- Integrity - Maintaining and assuring data accuracy, consistency and completeness.
- Authenticity - Ensuring data, transactions and communications are genuine.
- Non-Repudiation - Assuring neither party involved in a transaction denies having sent/received data.
- Accessibility & Availability - Ensuring data is available when required; Assuring that means to access data are present.

Almost one hundred security requirements were identified in the initial (analysis) phase of the REWARD project and implemented in the sub-sequent phases, always remembering the above mentioned Security Concepts & Principles and the operational objectives of project.

In terms of software technologies used for the implementation of the REWARD Security Framework, only mainstream open source and highly performance packages and computer language frameworks were used, namely:

- Java Technology[20] – Mobile, Standard and Enterprise Editions
- Microsoft Technology - .Net Framework[21] and Azure Cloud[22]
- Open Source Security Technology[23] – OpenSSL and JKS

[20] http://www.oracle.com/technetwork/java/index.html
[21] http://www.microsoft.com/net
[22] http://azure.microsoft.com/
[23] https://www.openssl.org/

Considering the binomial; collection of the identified security requirements and elected software technologies, a set of security functionalities was identified, designed and implemented (as a set of software components and packages) during the lifetime of the REWARD project. These functionalities were broken down into two main categories: Horizontal & Developed Ad-hoc Security Functionalities and together aimed the mitigation (avoidance) of a group of recognized ICT Security Threats (considering the objectives of the SOA architecture with mobile components of REWARD). The table below summarizes the complete list of Security Functionalities and Security Threats.

Security Functionality		**Security Threats**
Horizontal	**Developed (Ad-hoc)**	
Secured protocol	White List	Denial of Service
Security Certificates	Anti-Denial of Service (DoS)	Sniffing
TETRA Security	Offline Data Retention	Replay
High availability	Acknowledgement	Traffic Redirection
Firewall / Gateway	Anti-Cloning	Hijacking / Man In The Middle
Backups / Restore Plans	Digital Signature	Fraud (Id. theft)
Authentication & Authorization	Authentication & Authorization	Trojan Horse & Virus & Worms & Malware
Anti-Virus	Transaction and Error Logging and General Checking	Data Modification
		Compromised-Key

Table 1: Security functionalities and threats.

One of the strong requirements for the REWARD system network communications support was to consider both public mobile IP networks and private TETRA networks (e.g.: law enforcement and civil protection forces) on the mobile sensor tier.

The usage of either communication network is made seamlessly within the REWARD system, wherein the TETRA Network in-place security mechanisms are used off-the-shelve and a TETRA-to-IP driver was developed with the incumbency of translating the messages to the XML REWARD schema notation.

REWARD security functionality components and packages (i.e. the REWARD Security Framework) are deployed on each architectural tier (sensors, Tetra Driver, Middleware, Cloud and CMS) with the purpose of securing its communication channel, messaging interfaces and also its related infra-structure.

The architecture diagram depicted in Figure 22, generically, the deployment of the REWARD Security Framework among system tiers.

Writing this final report at the end of the REWARD project, one can state that all the proposed objectives for the work package 7 were successfully achieved, producing a technologically comprehensive Security Framework, adapted to the envisioned operational objectives of the REWARD system, and above all allows the following major added values & benefits:

- Documented set of security and configuration best practices

- Both Horizontal & Ad-hoc security components
- Solves / Mitigates security threats
- Easy integration & configuration
- Low computing overhead
- Scalable with the REWARD workload
- Gateway with TETRA networks
- Transparent and seamless usage on system operation
- Easily swappable horizontal components

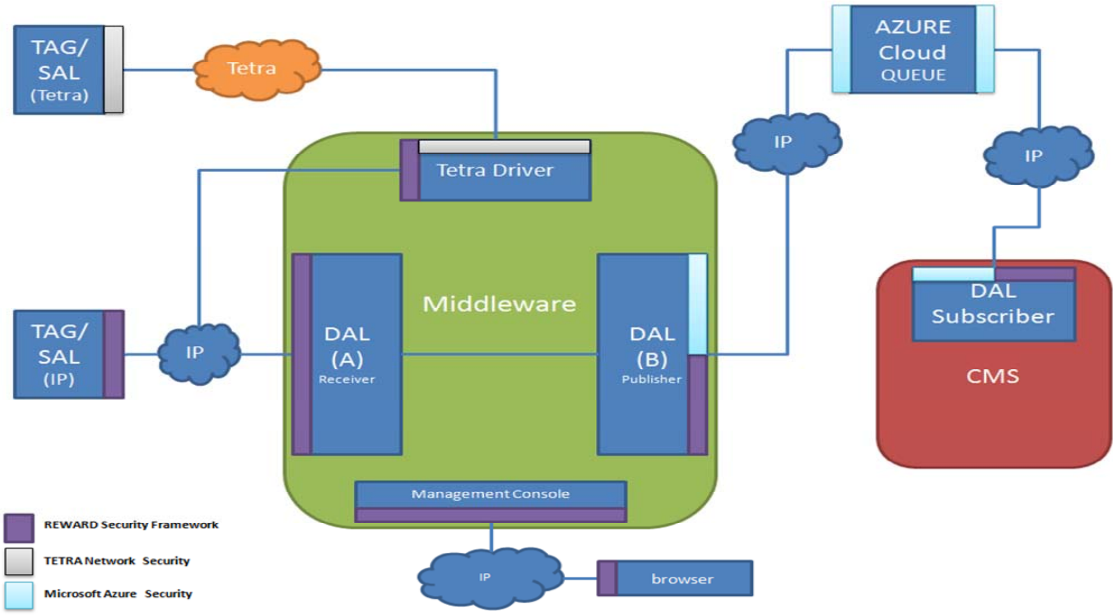


Figure 22: REWARD ICT Security Architecture

3.8 REWARD Validation

Through the synergy of all REWARD project partners, correspondence, call conferences, face-to-face and virtual meetings, the partners defined the scenarios for demonstration and test bed, as well as an accurate real test planning which includes the manipulation of real radioactive material in public space thanks to the collaboration of Italian Fire Brigades.

The test bed was successfully implemented following the three main stages: simulation, hardware-in–the-loop (HWIL) test and Real Sketching. The significant results achieved are those to get a functional test bed that provides a network of sensors that communicate via a wireless network with the middleware component which after processing the received data sends them, using Microsoft azure service bus, the component CMS which analyzes them, processes and presents on the console system results. Last but not least, the Security Framework is a horizontal and ad-hoc security measure integrated in the test bed.

Prior to real tests, the REWARD system was tested in a simulated environment using Radiological Environment Monte Carlo Simulation. Two scenarios were described and characterized: (i) an Improvised Nuclear Device (IND) and (ii) Radioactive Dispersal Device (RDD).

The first stage of the simulation work was related to the first scenario, the IND device. Geant4[24] was used to estimate the neutron detection efficiency of different sensor geometries, in order to determine the optimum design parameters for the sensors. The simulated neutron fluxes produced by an IND and the final neutron distribution in the sensors of REWARD's module were then presented. These values and the experimentally measured sensor efficiencies were combined to calculate the system response and estimate the minimum detectable activity.

The second stage consisted in simulating the second scenario, involving an RDD. Two alternative and complementary approaches were followed for this task:

1. MCNP6[25] was used to simulate a source-detector system representing the Goiânia accident. The results were benchmarked with experimental data taken from measurements in the laboratory. The response of the detection system was tuned to match the experimental results across the energy spectra.
2. Geant4 and MCNPX were used to simulate photon fluxes coming out of different encapsulated sources and RDDs. The response of the detection system was modeled with TCAD[26] simulation tools using the operational parameters of the CZT sensors. The minimum detectable activities and the detection limits were also estimated for each encapsulated source and RDD.

In the first approach, the benchmarks were, in general, satisfactory for energies above 100 keV. This was used to predict the response of the detector system in a scenario similar to the Goiânia accident, a 137Cs radiotherapy source with an activity of 50.9 TBq shielded by four different materials. The results, based on experimental data, predict that a car equipped with the REWARD system and passing close to such a source should be able to detect it and identify it, even for short exposure times.

The second approach, based on the simulation of the detector response using TCAD simulation tools, allowed the estimation of the minimum detectable activities and detection limits for different cases, without facing the difficulties related to statistics that arise in the first approach. From the simulation results, it was predicted that the REWARD system should be able to detect an RDD similar to the one from the Goiânia accident for distances up to a few hundred meters.

[24] S. Agostinelli et al. (Geant4 Collaboration),2003. *Geant4—a simulation toolkit*, Nucl. Instr. and Meths. A 506(3), pp. 250-303, doi:10.1016/S0168-9002(03)01368-8.
[25] MCNP6 Users Manual - Code Version 6.1.1beta, LA-CP-14-00745, June 2014.
[26] Sentaurus TCAD, Website: http://www.synopsys.com/Tools/TCAD

Overall, the simulation work provides an important estimation of the performance of REWARD's detection system in the presence of IND and RDD devices, which cannot be measured experimentally within the resources available during project development.

Testing is an essential part of the validation and verification process to ensure that "the right job is being done." Testing determines if the platform functions as intended within the target environment without performing any unintended or adverse functions. To obtain a satisfying outcome testing the test bed demonstrator, the activity was divided in two main parts: factory test and field test.

The factory tests are accomplished during a specific timeline:

- From M24 to M26: analyzes the CMS component not integrated with the others.
- From M27 to M29: analyzes the integration between all the REWARD components.
- From M30 to M32: M32 analyzes the situation awareness and data analysis functionality.
- From M33 to M35: analyzes the algorithms of localization and identification and data analysis.

All factory test were performed using the simulator, the first two factory test sections using simulated data, and the last two factory test sections using the data collected during the field tests of May 2014.

With regards to the integrated REWARD system tested in a real environment, two field tests were performed, the first one from 12th to 15th of May 2014 in Naples, and the second from 20th to 24th of October 2014. The second test included a public demonstration of the complete REWARD system and was held during REWARD's final workshop on 24th of October 2014. Figure 23 to Figure 25 were taking from the field test sessions. Figure 23 shows a tag during setup in Naples Civil protection premises, Figure 24 shows radioactive sources deployed (within premises of Naples Fire Brigades Headquarters), and Figure 25 shows one of the cars equipped with the REWARD tag.

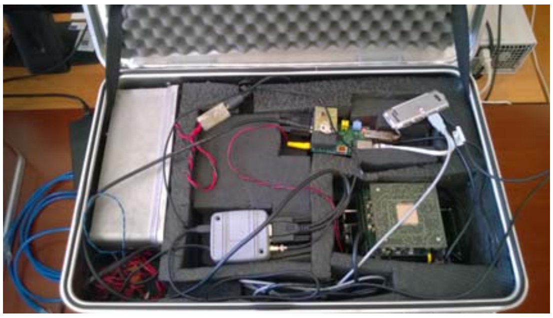


Figure 23: REWARD tag preparation for field tests

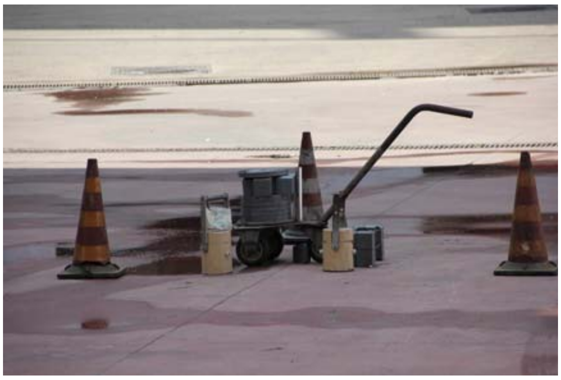


Figure 24: Radioactive sources deployed by the Rome Fire Brigades

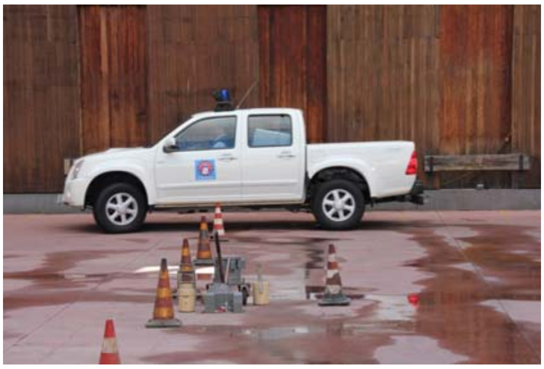


Figure 25: Civil Protection car equipped with the sensor tag passing near the radioactive sources in Naples fire brigades headquarters.

The first field test consisted of monitoring the environmental radiation within a controlled region of interest and studying the response of the system to different radiation sources (^{60}Co and ^{226}Ra) deployed in the area. Civil Protection of Campania Region (DIP) and the CBRN group of the Italian Fire Brigades, in collaboration with the REWARD's partners used two REWARD tags and deployed different radiation sources in a controlled public location to conduct the tests. During the first field test the radioactive background of the area was measured by the REWARD system, and the radiation levels as a function of the geographical location was recorded. Additionally, the background radiation map was created. The same exercise was repeated with the radiation sources deployed in order to evaluate the system's response. The results obtained were used to improve the system and prepare the second test phase and final demonstration.

During the final field test, radiation sources were deployed as in the first stage. All activities were performed imagining a real use scenario where several instances of the REWARD tag were installed in vehicles in an ordinary patrolling around the Headquarters of the Fire Brigades in Naples. The REWARD control room was installed within the Mostra d'Oltremare in Naples simulating a command and control centre. The CBRN group of the Italian Fire Brigades deployed different radiation sources. During the demonstration, the sources were detected and identified by the REWARD Central Monitoring System, triggering an alarm on the command and control centre operator interface. The whole process was filmed (the video will be uploaded in the project website) and the persons assisting to the final workshop could follow the whole process: detection, localization, and identification of radioactive sources in real time.

The outcome of the test results is that the REWARD system achieves the goals expected.

4 REWARD potential impact and the main dissemination activities and exploitation of results

4.1 REWARD potential impact

Homeland Security & Public Safety market is one of the most increasing market in terms of global business opportunities. The global radiation detection, monitoring and safety market for homeland security defence and the manufacturing industry were valued at $131.5 million and $83.6 million, respectively, in the year 2012 and it has been estimated that it could reach $546 billion by 2022. The radiation detector market stands at about $25 billion in 2013 and projected to grow at 4% annually over the next 8 years to about $33 billion. The market is divided into medical radiation detectors (66% market share), safety & monitoring (14%) detectors and specialty & custom detectors (20%). The report titled “Radiation Detection Materials Markets 2013” predicts that scintillation (crystalline and thin-film), semiconductor, and non-3He neutron detector materials revenues will grow from $2.3 billion (USD) this year to $3.7 billion in 2020. REWARD project will contribute to the growth of the security, monitoring and sensor technology industries and markets. REWARD provided a new tool for detecting difficult to detect radioactive sources and nuclear materials, reinforcing Europe’s leadership role on CBRN protection, as demonstrated by the expressions of interest received by REWARD for further pilots’ implementation trials, industrialization and commercialization purposes and further projects preparation. In fact, after an evaluation of existing commercial products and projects with similar features, it was noticed that REWARD excels, respect of most of the commercial systems, for the offered complete functionalities: both neutron and gamma, detection and identification of radioactive sources with good resolution over a wide energy range, multi sensors network, mobile, compact, easiness of installation, wireless communication module and data transmission, flexibility and customization of the Command and Control Center software/services.

The most relevant positive social impacts of REWARD are: improved public health and security, in terms of a reduction in casualties and long-term health problems related to RN incidents, the ability for authorities to disseminate information about REWARD when needed to reduce any localised levels of public fear and anxiety and an increased perception of safety.

REWARD can provide civil protection authorities and security forces with an operational tool for setting an effective early-warning system to be implemented for preventing accidents triggered by an uncontrolled management of radioactive sources. A REWARD-based early warning system could ensure societal and economic savings much more relevant than the costs required for its implementation and deployment at operational level. Also, thanks to its accuracy in critical event detection, the societal and economic loss due to false alarms is expected to be negligible.

One of the primary fields of operational application is the prevention of illegal or uncontrolled management of waste with radioactive sources. For instance, this scenario is of great concern in Italy, where local communities, opinion leaders and some environmental associations, also supported by some health data statistics, have attributed the increase of cancer-related mortality in some critical hot-spots to the illegal disposal of waste containing radioactive material. Due to the lack of scientific information concerning the actual spatial extend, the nature and the magnitude of this type of illegal disposal as well as its environmental effects, both the social and the economic impact of this controversial scenario is remarkable. For instance, looking at the Campania Region only, after uncontrolled and unverified information concerning the pollution of agricultural lands spread throughout the media, the orders for the agricultural products dropped by 30% in 2013[27], despite less than 1% of the cultivated land resulted contaminated[28]. Just to give some figures about the economic implications of this scenario, since year 2009 the Italian Government has been investing around 100 million euros per year (partially refunded by taxation at the expense of hazardous waste management companies) to set up an information system (named SISTRI) for tracking hazardous waste management[29]. A REWARD-based early warning system would be helpful not only as an additional tool for identifying the radioactive disposals, but also for recovering the trust of the public opinion with respect to the efficiency of environmental agencies, security forces and civil protection authorities in monitoring and preventing environmental crimes.

The REWARD project had also a positive effect on governance, as the project result enhanced institutional cooperation and communication, improving information flows and helping to establish protocols, through:

- Better mapping of existing international cooperation and coordination mechanisms addressing CBRN issues;
- Increased cooperation with relevant agencies at international, EU and national level;
- Improved identification and exchange of good practices with international, European and national partners;
- Improved communication with the users of the system.

During the REWARD meeting, the Italian and Spanish civil protection authorities provided their expert opinions about the optimal strategies for integrating the REWARD system within a civil emergency management plan, particularly for what concerns the preparedness and response actions. The Italian Fire Brigades, by means of several real-case studies, pointed out to the REWARD project partners some relevant features that a mobile radiation surveillance should have for its effective usage at operational level. During the final project workshop, an IAEA representative highlighted the ethical implications concerning the acquisition of environmental data that are relevant for the public safety.

4.2 REWARD dissemination activities and exploitation of results

The expressions of interest received in the last months of the project from the end users (Security Forces), from industries (dealing with CBRNe detection and Security interested in the REWARD

[27] www.ilmattino.it/salerno/agricoltura_commesse_gi_del_30_effetto_terra_dei_fuochi_anche_a_salerno/notizie/337877.shtml;

[28] https://geograficamente.wordpress.com/2014/03/14/terra-dei-fuochi-tra-napoli-e-caserta-a-rischio-solo-il-2-per-cento-del-territorio-i-rifiuti-speciali-e-tossico-nocivi-delle-industrie-del-nord-italia-ed-europa-li-abbandonati-in-discar/

[29] http://it.wikipedia.org/wiki/Sistema_di_controllo_della_tracciabilit%C3%A0_dei_rifiuti

commercialization) and from other projects’ coordinators (having invited the REWARD partners to participate to follow up projects) represent the most important result related to the dissemination and exploitation activities. In function of those expressions of interest, the exploitation plan and business model were developed, updated and optimized. The REWARD exploitation plan is focused on the system commercialization. The IPR of the project results are protected by the Consortium Agreement and by the ownership distribution defined in the Deliverable D8.4. The current REWARD exploitation plan foresees the organization of further pilots, a development phase to proceed with the industrialization of the prototypes and ICT services developed in the project and the participation to initiatives like Fast Tracking to Innovation and other H2020 EC funding schemes for the preparation of follow up projects.

The active participation of the partners to many industrial events, exhibitions, meetings with stakeholders and the organization of two REWARD workshops allowed establishing contacts, collaborations and relationships with end users, stakeholders and EU funded projects covering similar problems. In particular, around 50 participants (Figure 26) attended the REWARD Final workshop including EC projects’ coordinators and partners, research centres and institutions dealing with nuclear radiation detection, industries and several representatives from Security Forces. The active participation of Civil Protection of Campania region, the Italian Fire Brigades, the Spanish Guardia Civil and other international stakeholders ensured the success of those workshops.

Figure 26: Participants of the REWARD Final workshop - 24th October 2014

Figure 27: NCT CBRNe Innovation Award 2013

Some of the most effective dissemination activities carried out in the project include the maintenance and update of the project website, several press releases in newspapers and magazines related to REWARD topics, the award received by the project at the NCT CBRNe Innovation Awards 2013 (Figure 27), the preparation and distribution of promotional materials like Newsletters, Press Kits and two REWARD videos, one summarizing the project features and the other focused on the demo with on field testing campaign organized during the Final workshop.

The scientific dissemination was carried out through the publication of 2 peer-reviewed articles and 3 papers published in peer-reviewed Book of Proceedings of recognized international conference like IEEE NSS/MIC/RTSD, SPIE Optics and Photonics and the Iberian Conference on Information Systems and Technologies. Oral and poster presentations were delivered in high-profile international scientific conferences and events such as: NEUDOS12: Neutron and Ion Dosimetry Symposium, 10th International Conference on Position Sensitive Detectors, 1st International Conference on Dosimetry and its Applications and the EGU General Assembly. A total of 6 articles were published in the specialized press (5 in Security and Defence, 1 in Smart Cities). Finally, 2 PhD thesis have been published by the Albert-Ludwigs-University of Freiburg and CSIC.

A PowerPoint presentation was developed to summarize the project results and to be used for presenting the project to potential investors and customers. The document is built to be addressed to general public, with simple and visual contents. The results of the validation phase, included in the presentation, contribute to convince potential investors about the status of maturity of the project; similarly the list of expressions of interest already received by end users, industries and other external partners demonstrates the sustainability of the project after its end.

REWARD Website: http://www.reward-project.eu/

Link to REWARD videos:

- https://www.youtube.com/watch?v=Ys3Oe041phU

Link to some of the REWARD publications:

- D.O.I. 10.1088/1748-0221/9/12/C12006

- D.O.I. 10.1109/CISTI.2014.6876872
- D.O.I. 10.1088/1748-0221/9/04/P04010
- http://www.cbrneportal.com/reward-project-security-on-the-road/

Table 2 contains photos of dissemination events:

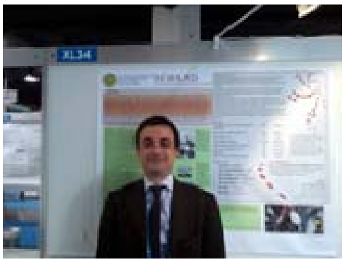
 Dr. Mauro Biafore (DIP) at the EGU GA 2012	 REWARD at CSCM Exhibition area	 Mr. Folco de Luca Gabrielli (delegate from VCT) interviewed at the NCT CBRNe Innovation Award
 Prof. Manolo Lozano (CSIC) at the SCINTILLA workshop	 XIE stand at NSS-MIC 2013	 Massimo Guadagnoli presenting REWARD to the Prince of Kent (cousin of Queen Elisabeth the 2nd).
 1st REWARD open workshop	 S&C Stand at MWC 2014	 REWARD at NCT CBRNe Europe 2014

Table 2: REWARD dissemination events pictures