bimestrale dell'ENEA
anno 60

Speciale

ENEA TECHNOLOGIES FOR SECURITY

SPECIALE I - 2014

**Energia, Ambiente
e Innovazione**

Speciale

ENEA technologies for security
A cura di Roberta Fantoni, e Paolo Di Lazzaro

Registrazione
Tribunale Civile di Roma
Numero 148 del 19 aprile 2010 del Registro Stampa

Direttore Responsabile
Diana Savelli

Comitato di Direzione
Pietro Agostini, Vincenzo Artale, Giacobbe Braccio, Marco Casagni, Gian Piero Celata, Vincenzo Cincotti, Carlo Cremisini, Pierino De Felice, Roberta Delfanti, Nino Di Franco, Francesco Di Mario, Roberta Fantoni, Elena Fantuzzi, Massimo Forni, Massimo Iannetta, Riccardo Levizzari, Carmela Marino, Paride Meloni, Silvio Migliori, Roberto Morabito, Aldo Pizzuto, Vincenzo Porpiglia, Sergio Sangiorgi, Massimo Sepielli, Leander Tapfer, Ezio Terzini, Carlo Tricoli, Marco Vittori Antisari, Gabriele Zanini

Comitato tecnico-scientifico
Osvaldo Aronica, Ilaria Bertini, Paolo Clemente, Paolo Di Lazzaro, Andrea Fidanza, Stefano Giammartini, Giorgio Graditi, Massimo Maffucci, Laura Maria Padovani, Paolo Ruti, Emilio Santoro

Coordinamento editoriale
dei fascicoli: Giuliano Ghisu
di questo speciale: Antonino Dattola

Collaboratori
Daniela Bertuzzi, Paola Carrabba, Sergio Cappucci, Orietta Casali, Antonino Dattola, Barbara Di Giovanni, Giovanni Puglisi

Traduzioni e revisione lingua inglese
Carla Costigliola

Progetto grafico
Paola Carabotta, Bruno Giovannetti

Edizione web
Antonella Andreini, Serena Lucibello, Concetta Manto

Promozione
Paola Crocianelli

Per informazioni e contatti: infoeai@enea.it

Pre-stampa
FGE Srl - Fabiano Gruppo Editoriale
Regione Rivelle, 7/F – 14050 Moasca (AT)
e-mail: info@fgeditore.it

Stampa
Varigrafica Alto Lazio
Via Cassia, km 36,300 (Zona industriale)
01036 Nepi (VT)

Finito di stampare nel mese di gennaio 2015

Prodotto realizzato impiegando carta Symbol Freelife certificata FSC

I-2014

2 **Foreword**
R. Fantoni, P. Di Lazzaro

Sp ENEA technologies for security

SCENARIO

4 **Security concept and threat's scenarios: New technologies and social security**
Il concetto di security e gli scenari di minaccia: le nuove tecnologie e la security sociale
R. Fantoni, A. Palucci

17 **New technologies and police activities: Security and forensic issues**
F.S. Romolo, G.G. Vadalà

EXPLOSIVE DETECTION

23 **Explosive's trace detection by laser-induced breakdown spectroscopy**
V. Lazic, A. Palucci

30 **Raman spectroscopy for detecting of trace amounts of energetic materials for counterterrorism issues**
S. Almaviva, F. Angelini, R. Chirico, G. Dipoppa, I. Menicucci, M. Nuvoli, A. Puiu, A. Palucci, S. Botti, L. Cantarini, A. Rufoloni

39 **Differential Absorption Lidar detection of explosive precursors by Optical Parametric Oscillator laser systems**
A. Puiu, L. Fiorani, R. Borelli, M. Pistilli, O. Rosa, A. Palucci

49 **Scanning Lidar fluorosensor for detection in a post blast scene of plastic debris coming from components of Improvised Explosive Devices**
L. Caneve, F. Colao, I. Menicucci, A. Palucci, M. Pistilli, V. Spizzichino, G. Terranova

BIOHAZARD

56 **Innovative devices for biohazards and food contaminants**
A. Lai, S. Almaviva, V. Spizzichino, L. Addari, G. Giubileo, G. Dipoppa, A. Palucci

CRITICAL INFRASTRUCTURES

64 **Decision Support System aimed at improving the "physical protection" of critical infrastructures against natural events**
A. Di Pietro, L. La Porta, M. Pollino, V. Rosato, A. Tofani

71 **Quality of Service of an electrical grid under cyber attacks to its supervisory control and data acquisition system**
E. Ciancamerla, B. Fresilli, M. Minichino, S. Palmieri, T. Patriarca

80 **Underwater security: Self organising systems**
C. Moriconi, R. Dell'Erba, S. Betti

Indice

NUCLEAR

89 **The Nuclear Security Summit process: The turn of the screw**
Il processo del Nuclear Security Summit: il giro di vite
F. Padoani

102 **The European EDEN project: Thematic Demo on 3D laser inspection in a nuclear reactor**
L. De Dominicis, A. Palucci, M. Carta, M. Ferri de Collibus, R. Fantoni, G. Fornetti, M. Francucci, M. Guarneri, M. Nuvoli, M. Palomba, E. Santoro, M. Sepielli

108 **Marking and tracking radioactive materials: A possible hi-tech solution**
S. Bollanti, P. Di Lazzaro, F. Flora, L. Mezi, D. Murra, A. Torre, F. Bonfigli, R.M. Montereali, M.A. Vincenti

114 **Facing dispersion of radioactive material: ENEA's skills**
S. Sandri

TRAINING

121 **New frontiers of safety and security: Chemical, Biological, Radiological, Nuclear, explosive events**
A. Malizia, V. Cusmai, V. Rossi, T. Labriola, E. Farrugia, F. Campopiano, F. Salerno, V. Trombadore, L. Cadoni, G. Rezza, R. Fantoni, S. Sandri, M. Chiappini, A. Gucciardino, F. D'Amico, C. Russo, D. Rothbacher, M. Carestia, D. Di Giovanni, O. Cenciarelli, C. Perrimezzi, I. Palombi, C. Bellecci, P. Gaudio

129 **Developing the human dimension of security by means of Centres of Excellence**
F. Padoani, A. Rizzo

138 **Building a Chemical, Biological, Radiological, Nuclear, explosive events Tech Advisor and First Responders to support top decision makers during emergencies**
L. Palombi, C. Belleccia, A. Malizia, V. Cusmai, V. Rossi, T. Labriola, E. Farrugia, F. Campopian, F. Salerno, V. Trombadore, L.Cadoni, G. Rezza, R. Fantoni, S. Sandri, M. Chiappini, A. Gucciardino, F. D'Amico, D. Rothbacher, M. Carestia, D. Di Giovanni, O. Cenciarelli, C. Russo, C. Perrimezzi, P. Gaudio

Foreword/Prefazione

Roberta Fantoni, Paolo Di Lazzaro

Since September 11, 2001, a large concern has spread worldwide about Security, meaning by this term the degree of protection from any harm or danger. The need to defend citizens against potential, extremely violent terroristic attacks stimulated institutions to take all conceivable preventive measures. In parallel, the consciousness of the risk pushed national and international organizations to support research addressed to the development and application of innovative technologies more and more adequate to counteract this kind of threats. The use of early warning devices (e.g., detectors, sensors) was considered either alone or in suitably designed networks, and the development of advanced tools for intervention (e.g., robotics, remote handling) was envisaged.

ENEA, with its consolidated technology background and unique competences on handling nuclear hazard, has been involved since the early beginning in the development of innovative tools for Security. The topics considered include contrast to terrorism based on Chemical, biological, radiological, and nuclear defense (CBRN) weapons, recently including Improvised Explosive Devices and “dirty bombs” (CBRNe), and the protection of critical infrastructures, with special attention to power production plants and energy distribution networks.

In the international panorama ENEA acts in close contact with the international institutions (EC, NATO, EDA), sitting in networks of excellence, to support with its expertise the upgrading of present legislation, and technologically contributes to specific projects (from capability to demonstration). Along with these

L’evento dell’11 Settembre 2001 è stato motivo di grande riflessione e preoccupazione in tutto il mondo in merito alla *security*, intendendo con tale termine il grado di protezione da qualunque danno o pericolo volutamente indotto da agenti esterni e/o terroristi. La necessità di difendere i cittadini contro potenziali attacchi terroristici estremamente violenti ha spinto le istituzioni a prendere tutte le misure preventive possibili. Parallelamente, la coscienza del rischio ha fatto sì che le organizzazioni nazionali e internazionali supportassero la ricerca mirata allo sviluppo e all’applicazione di tecnologie innovative sempre più efficaci nel contrastare questo tipo di minacce. È stato presa in considerazione la possibilità di disporre di dispositivi di preallarme (ad es., rilevatori, sensori), da utilizzare da soli o all’interno di reti appositamente progettate, ed è stato previsto lo sviluppo di strumenti avanzati di intervento (ad es., robotica, gestione remota).

Con la sua consolidata esperienza tecnologica e le sue competenze uniche nella gestione del pericolo nucleare, l’ENEA è stata coinvolta fin dall’inizio nello sviluppo di strumenti innovativi per la security. Gli aspetti considerati comprendono il contrasto al terrorismo basato su armi CBRN (chimiche, biologiche, radiologiche e nucleari), che includono i più recenti IED (Improvised Explosive Devices) e le cosiddette “bombe sporche” (CBRNe), e la protezione di infrastrutture critiche, con particolare attenzione alle centrali elettriche e alle reti di distribuzione di energia elettrica.

Nel panorama internazionale, ENEA agisce a stretto contatto con gli organismi internazionali (EC, NATO, AED), nell’ambito di reti di eccellenza, mettendo a disposizione la propria competenza per l’aggiornamento technological activities, ENEA collaborates with many groups at the national and international levels, including SMEs and large industries, and with special corps of the Italian Army. In order to share a common language needed during interventions, ENEA plays a role in the gift basket for the EU CBRN Centre of Excellence (CoE) initiative and takes part in the organization of the CBRNe master promoted by The University of Rome Tor Vergata.

This special issue of EAI offers an overview of the major current ENEA activities related to Security, stressing the external cooperation that shares the final goal focused on developing technologies for a broad range of specific tasks, from the intervention to forensic aspects. After an introduction where the concept of Security is explained, mostly referring to scenarios of current European interest, contributions are presented along an ideal path that starts with CBRNe risks, focusing first on sensors for explosives and their chemical precursors, then on bio-hazard detection. The development of technology and tools is primarily considered for field use, including post-blast in situ analysis for forensic application. Specific tools for interventions to protect selected critical infrastructures are presented, including harbors and energy distribution networks.

The other scenario, dealing with nuclear and radiologic risks, is then explicitly considered at the international level: peculiar examples of specific sensors, operational protocols and technological countermeasures are presented. Finally, the importance of education and training on the multidisciplinary fields related to Security is addressed in relation to existing European excellence centers and on-going dedicated master courses.

As in any short anthology, the available space does not allow for an exhaustive treatment of each topic. However, we are confident to give to the reader a taste of the most significant developments at the international level, which are currently on-going at ENEA.

della normativa e apportando il proprio contributo tecnologico in progetti specifici (dalla capacità alla dimostrazione). Oltre tutte queste attività tecnologiche, l'ENEA collabora con molti gruppi in ambito nazionale e internazionale, incluse le PMI e le grandi industrie, anche insieme a corpi speciali dell'esercito italiano. Al fine di condividere un linguaggio comune necessario durante gli interventi, l'ENEA svolge un ruolo importante nel paniere delle iniziative del EU CBRN Centre of Excellence (CoE) e partecipa all'organizzazione degli International CBRNe Master Courses promossi dall'Università di Roma Tor Vergata.

Questo numero speciale di EAI offre una panoramica delle maggiori attività per la *security* attualmente svolte dall'ENEA, evidenziando la cooperazione esterna che condivide l'obiettivo finale di sviluppare tecnologie per una vasta gamma di compiti specifici, dall'intervento sul campo agli aspetti forensi. Dopo una breve introduzione al concetto di security negli scenari di attuale interesse europeo, i contributi presentati dagli autori seguono un percorso ideale che inizia con i rischi CBRNe, incentrandosi prima sui sensori per esplosivi e i relativi precursori chimici e poi sul rilevamento di materiali biologici pericolosi. Lo sviluppo di tecnologie e strumenti viene considerato principalmente per l'uso sul campo, inclusa l'analisi post-esplosione in loco per applicazioni in area forense. Sono inoltre illustrati gli strumenti specifici di intervento per proteggere infrastrutture critiche, inclusi i porti e le reti di distribuzione di energia elettrica.

L'altro scenario, relativo ai rischi nucleari e radiologici, viene esplicitamente preso in considerazione a livello internazionale, riportando esempi di sensori specifici, protocolli operativi e contromisure tecnologiche. Infine, l'importanza dell'istruzione e della formazione multidisciplinare relative alla security viene esposta in relazione ai centri di eccellenza europei e ai master universitari dedicati esistenti.

Come in qualunque breve antologia, lo spazio disponibile non consente di trattare ciascun argomento in maniera esaustiva. Tuttavia, siamo convinti di essere riusciti ad offrire al lettore un assaggio degli sviluppi più significativi a livello internazionale, attualmente in corso presso e ad opera dell'ENEA.

traduzione di Carla Costigliola

Il concetto di Security e gli scenari di minaccia: le nuove tecnologie e la Security sociale

Il presente articolo descrive brevemente il concetto di security, il suo significato attuale e le implicazioni che derivano dalla sua applicazione. Le minacce più probabili vengono prese in esame, passando in rassegna gli agenti biologici e chimici utilizzati in situazioni di conflitto, e considerando gli esplosivi assieme ai relativi precursori, questi ultimi particolarmente adatti alla costruzione di dispositivi esplosivi improvvisati (IED, Improvised Explosive Devices). Sono inoltre illustrate tutte le minacce di tipo CBRNe (chimiche, biologiche, radiologiche, nucleari ed esplosive) ed è brevemente spiegato l'incubo della "bomba sporca".
Vengono quindi descritte le attività di ricerca e sviluppo tecnologico per la security, così come previste a livello europeo nei programmi attuali e precedenti, a livello sia internazionale che italiano. Infine, alcuni scenari di riferimento, con particolare attenzione alla security del trasporto di massa, sono qui esposti con particolare riguardo ai casi in cui lo sviluppo tecnologico potrebbe diventare più efficace nell'immediato futuro.

Security concept and threat scenarios: New technologies and social security

The concept of security with its current meaning and the implication of its implementation are shortly introduced here. A threat analysis is presented reviewing biological and chemical warfare agents, explosive compounds and their precursors, the latter being suitable to the construction of improvised explosive devices (IED). All Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) threats are considered, and the "dirty bomb" nightmare is introduced.
Research and Technology Development (RTD) for Security is discussed as foreseen at the European level, in both former and current programs, as well as at a higher international level and in the Italian surroundings.
Reference scenarios, with special attention to mass transport security, are discussed trying to foresee where technology development might become more and more effective in the near future.

DOI: 10.12910/EAI2014-85

R. Fantoni, A. Palucci

Contact person: Roberta Fantoni
roberta.fantoni@enea.it

Il concetto di Security

Con il termine Security si fa riferimento al grado di protezione da qualunque tipo di danno o pericolo. Tale concetto è applicabile a qualunque bene vulnerabile e di valore: singoli individui, una comunità, una nazione o un'organizzazione. Il concetto di security viene generalmente associato al rischio, cioè alla possibilità che si verifichi un evento dannoso, e alla minaccia, l'azione che rende il rischio una realtà concreta. I sistemi di security dovrebbero tenere adeguatamente conto dei rischi e contrastare le minacce. Nella maggior parte dei sistemi di security, l'anello più debole della catena è quello più importante. Le minacce terroristiche sono tipicamente asimmetriche, poiché il "difensore" deve coprire tutti i punti di possibile attacco, mentre l'"attaccante" ha solo bisogno di individuare un punto debole sul quale concentrare gli sforzi perturbatori.

Ad ogni campo di azione corrisponde uno specifico problema di security. Un esempio di possibile lista di aspetti relativi alla security potrebbe essere il seguente:

- *Information Technology (IT): security per applicazioni, sistemi informatici, dati, informazioni, reti.*
- *Security fisica: aeroporti e porti, filiera alimentare e approvvigionamenti, case, infrastrutture, scuole, centri commerciali, beni culturali, aree sportive.*
- *Security politica, sociale e monetaria: sicurezza nazionale, internazionale, pubblica, finanziaria.*

Il presente articolo prende in esame gli aspetti fisici della security, in particolare quelli relativi ai progressi delle attività di ricerca e sviluppo tecnologico.

Storicamente i diversi aspetti della security sono stati trattati singolarmente, in genere da diversi operatori pubblici o privati dotati di dipartimenti specificamente dedicati alla security per sistemi IT, protezione fisica e prevenzione di frodi. Oggi è generalmente riconosciuta una correlazione dei requisiti per la security e viene preferibilmente seguito un approccio olistico, che comporta una gestione del rischio integrata di tipo "all hazards". La convergenza delle discipline della security verso questo tipo di approccio ha avuto ampio impulso dallo sviluppo delle tecnologie di videosorveglianza digitale, dalla digitalizzazione e dalle reti di sistemi fisici di controllo, quali, ad esempio, i sistemi SCADA (Supervisory Control And Data Acquisition) di controllo, supervisione e acquisizione dati [1].

The concept of Security

Security is the degree of protection from any harm or danger. It applies to any vulnerable and valuable asset, such as single persons, community, nation, or organization. The concept of Security is usually associated with risk, i.e. the possibility that some hazardous events concretize, and with threat, i.e. the action that triggers the risk actualization. Security systems should adequately take risks into account and counteract threats. In most security systems, the "weakest link in the chain" is the most important. Terroristic threats are usually asymmetric since the "defender" must cover all points of possible attack, while the attacker only needs to identify a single weak point upon which to concentrate the disruptive efforts.

Different realms can be considered dealing with specific security problems. An example of possible security categorization is given in the following:

- *Information Technology (IT) aspects:* Application security, Computing security, Data security, Information security, Network security.
- *Physical aspects:* Airport and port security, Food and Supply chain security, Home security, Infrastructure security, School security, Shopping center security, Cultural Heritage and Sport area security.
- *Political, social and monetary aspects:* Homeland security, Human security, International security, National security, Public security, Financial security.

This paper is focused on the physical aspects of security, in particular dealing with possible security improvements expected from RTD activities.

Various aspects of security were historically addressed separately, usually by different public or private operators with specific departments for IT security, physical security, and fraud prevention. The interconnected nature of security requirements is nowadays generally recognized, and a holistic approach to security, involving an "all hazards" management, is preferentially followed. The convergence of security disciplines into an integrated approach to Security was largely pushed by the development of digital video surveillance technologies and by the digitization and networking of physical control systems (e.g., by Supervisory Control And Data Acquisition systems - SCADA) [1].

A picture of the complexity of Security needs to consider the players, that take decisions and perform actions, the technological tools adopted to prevent or fight the threats, the technology developers whose role is to study and build these tools.

The main players are:

- government authorities, mostly concerned with political and social issues,
- the army, involved in military operations at the borders as well as in

Per avere un quadro della complessità della security occorre considerare gli attori, cioè coloro che prendono le decisioni e le attuano, gli strumenti adoperati per prevenire o combattere le minacce e gli sviluppatori di tecnologie, che hanno il compito di studiare e realizzare tali strumenti.

Gli attori principali sono:

- *le autorità di governo, che si occupano soprattutto di problematiche politiche e sociali;*
- *l'esercito, coinvolto in operazioni militari al confine e in interventi specifici in caso di catastrofi nazionali su larga scala;*
- *corpi civili pubblici (vigili del fuoco e protezione civile);*
- *corpi di polizia, per interventi di routine contro il terrorismo e il crimine organizzato.*

Creare opportune interazioni tra gli attori della security a livello nazionale e internazionale è una sfida oggi esplicitamente tenuta in grande considerazione, come dimostrano i tanti Master Courses di specializzazione nella security, tenuti nella maggior parte dei paesi industrializzati [2, 3].

Passiamo ora alla disamina degli strumenti disponibili per contrastare le minacce. È ben noto che lo spazio e la difesa nazionale siano universalmente ritenuti i principali propulsori dello sviluppo di nuove tecnologie. La duplice applicazione (militare e civile) delle tecnologie per la security ha sicuramente tratto beneficio dalle principali ricadute della ricerca in campo militare. Ad esempio, gli strumenti tecnologici sviluppati per la protezione di un accampamento militare in uno scenario bellico, quali sistemi di videosorveglianza, visione notturna, riconoscimento biometrico, possono essere utilizzati per la protezione di infrastrutture critiche (vedi, ad es., [4]). La crittografia è un ulteriore esempio di ricaduta tecnologica: originariamente sviluppata per proteggere le telecomunicazioni durante la seconda Guerra mondiale, è oggi alla base dei protocolli informatici di comunicazione e di scambio digitale di dati.

Gli sviluppatori di tecnologie rappresentano il terzo elemento critico di cui tenere conto nell'organizzazione di un sistema di security per la difesa nazionale. Se da un lato è estremamente necessario indirizzare la ricerca verso dispositivi rapidi, sensibili e selettivi per il rilevamento di possibili minacce aree, riducendo al massimo l'interferenza con le attività ordinarie ivi portate avanti, dall'altro i terroristi si evolvono parallelamente, perlopiù acquisendo le informazioni pubbliche disponibili, che consentono loro di mettere a punto minacce più

specific interventions for large-scale national disasters,

- non-military public organization (such as firemen and civil protection),
- the police, for routine interventions counteracting terrorism and organized crime.

To apply an appropriate interaction among security players, both at the national and international level, is a challenge explicitly considered nowadays in the security specializations master courses held in the most industrialized countries [2, 3].

The available tools to counteract the threats are the next issue. It is well known that space and army are worldwide acknowledged as the main drivers of technology developments. Security implementations may profit of major fallouts from military research, as far as dual technologies (military/civilian) are concerned. For instance, the technology tools developed to protect a military camp in a war theatre may be successfully utilized for critical infrastructure protection (video surveillance, night view, biometric recognition, etc.) see, e.g., [4]. As a further example, we can mention cryptography, first developed to protect telecommunication during World War II and nowadays at the basis of computer secure communication protocols and digital data exchange.

Technology Developers represent the third critical element in organizing a Security Homeland system. On the one hand it is really necessary to address research towards fast, sensitive and selective devices for detection of potential threats in crowded areas, minimizing the interference with the ordinary activities there carried on. On the other hand, terrorists evolve in parallel, mostly through public available information which allows them to choose more sophisticated threats or adopt new weapons (e.g., plastic knives to fool metal detectors, liquid precursors to be mixed on board for quickly assembling IEDs) [5].

Threat analysis

Biological (B) and chemical (C) warfare agents

Biological terrorism dates as far back as ancient Roman civilization, but now it is a primary concern in the States' political agendas. According to the Global Terrorism Database (GTD) of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) [6], biological and chemical attacks account for nearly 0.2% of terror attacks perpetrated worldwide between January 1st, 1970 and December 31st, 2011 [7]. Despite the ban, Weapons of Mass Destruction (WMD) have actually been used in warfare, as in the Iran-Iraq war in 1984/88: Iraq made use of chemical warfare agents [8] and in some terroristic attacks. Not only do biological agents affect specific targets but they can also potentially induce mass hysteria on the society exposed to them [9]. Malicious letters containing Bacillus anthrax, addressed in the U.S. to *sofisticate o di utilizzare nuove armi come, ad esempio, coltelli di plastica non rilevabili dai metal detector, precursori in forma liquida da miscelare una volta a bordo per assemblare rapidamente dispositivi esplosivi improvvisati, i cosiddetti IED (Improvised Explosive Devices) [5].*

Analisi della minaccia

Agenti chimici per guerra biologica (B) e chimica (C)

Sebbene il terrorismo biologico risalga ai tempi dell'antica civiltà romana, oggi rappresenta il principale elemento di preoccupazione all'ordine del giorno nell'agenda politica dei vari stati. Secondo il Global Terrorism Database (GTD) del National Consortium for the Study of Terrorism and Responses to Terrorism (START) [6], gli attacchi biologici e chimici equivalgono a circa lo 0,2% degli attacchi terroristici perpetrati in tutto il mondo tra l'1 Gennaio 1970 e il 31 Dicembre 2011 [7]. Malgrado siano state bandite, in realtà le armi di distruzione di massa (WMD) sono state usate in scenari bellici quali, ad esempio, la guerra tra Iran e Iraq nel 1984/88: l'Iraq ha fatto uso di sostanze chimiche [8] durante la guerra e in occasione di alcuni attacchi terroristici.

Tali sostanze biologiche non solo colpiscono obiettivi specifici, ma possono anche potenzialmente portare a fenomeni di isteria di massa nella società ad esse esposta [9]. Lettere contaminate, contenenti il bacillo dell'antrace, sono state spedite negli Stati Uniti a diversi uffici di testate giornalistiche e a due senatori dell'ala democratica, uccidendo cinque persone e infettandone altre 17 [10].

Negli ultimi cinque anni, il traffico illegale di merci, persone e sostanze ha portato ad accrescere fortemente il livello di controllo contro gli attacchi terroristici, in particolare contro la contaminazione biologica delle merci [11]. L'adozione di questo tipo di misure di security diventa di primaria importanza in aree al confine come, ad esempio, le aree portuali, dove meno del 5% dei container sono analizzati allo scanner e merci potenzialmente contaminate da sostanze biologiche vengono consegnate tramite una intricata catena di distribuzione. Tuttavia, anche altre strutture civili strategiche possono costituire un facile obiettivo: metro, supermarket, reti di distribuzione idrica.

I nuovi strumenti tecnologici devono essere mirati al rilevamento e al riconoscimento a distanza di diversi materiali biologici pericolosi (bat-

several news media offices and two Democratic Senators, killed five people and infected 17 others [10].

During the last few years, the flow of illegal goods, people and substances has strongly forced to increase the level of control against terrorist attacks, in particular for infection of goods with biological agents [11]. This is a primary need in the border security area, i.e. harbors, where less than 5% of containers are scanned and the goods, possibly contaminated by biological attack, are distributed in a tangled supply chain. Nonetheless, other strategic civil structures (metro, supermarkets, hydric supply chains, etc.) can be affected, too.

The technology tools to be developed are addressed towards the stand-off detection and recognition of different dangerous biological materials (bacteria and viruses), tracing their presence in the air. Noxious B-agents to be considered for bio-terrorism are in the most dangerous class A, like Bacillus anthracis (Anthrax), Yersinia pestis (pneumonic plague), and Variolavirus (Smallpox).

Chemical warfare agents are gases, such as Yperite (from World War I). Nevertheless, gases are nowadays seldom used by terrorists. A remarkable exception was the attack with sarin gas at the Tokyo metro in 1995 [12].

teri e virus), tracciandone la presenza nell'aria. Agenti biologici nocivi da considerare in caso di bioterrorismo sono quelli di classe A, quella più pericolosa: Bacillus anthracis (antrace), Yersinia pestis (peste), e Variolavirus (vaiolo).

Le sostanze usate per la guerra chimica sono gas come l'iprite, utilizzata per la prima volta durante la Prima Guerra Mondiale. Tuttavia, attualmente i gas non sono usati spesso dai terroristi, eccezione esemplare fu l'attacco alla metropolitana di Tokio, perpetrato con gas sarin nel 1995 [12].

Esplosivi e precursori (inclusi IED e bombe sporche)

La definizione comunemente usata per il termine esplosivo è: un materiale, o singola sostanza pura, o una miscela di sostanze, in grado di generare un'esplosione mediante la sua stessa energia. Solitamente gli esplosivi sono specie chimicamente stabili che richiedono uno stimolo esterno, come un colpo o una scintilla, per liberare la propria energia. I vari stimoli ai quali rispondono gli esplosivi e le modalità di risposta nel produrre esplosioni forniscono una base conveniente per la loro classificazione. In alternativa, si utilizzano classificazioni basate sulla composizione chimica, in particolare sulla presenza di un gruppo nitrogenato attivo (NO, NH, C-N etc.) o perossido (O-O).

Sebbene le minacce CB abbiano un forte impatto sui media e sulla mente della popolazione, lo strumento preferito in assoluto dai terroristi resta sempre l'uso di armi esplosive, principalmente perché sono economiche, disponibili dappertutto e relativamente semplici da maneggiare. Il database START [6] riporta attacchi con bombe per circa il 49% degli atti terroristici perpetrati in tutto il mondo tra l'1 Gennaio 1970 e il 31 Dicembre 2011, vedi Figura1. La figura mostra chiaramente i problemi sorti a seguito dell'evento dell'11 Settembre, che ha scatenato una escalation di attacchi esplosivi.

La maggior parte degli esplosivi sono caratterizzati da una pressione di vapore bassissima e persino rilevatori altamente sensibili di tracce di gas non riescono a reagire alla loro presenza. La prima sfida tecnologica per la security è stata riconosciuta nella possibilità di rilevare con rapidità e affidabilità tracce di esplosivo nei punti di transito (varchi in aree affollate), al fine di sostituire l'unico rilevatore di gas naturale sensibile e selettivo: il naso del cane. Il rilevamento spettroscopico della composizione degli

Explosives and precursors (including IED and dirty bombs)

A common definition of explosive is: a material, either a pure single substance or a mixture of substances, which is capable of producing an explosion by its own energy. Explosives are usually chemically stable species which commonly require some stimulus, like a blow or a spark, to liberate their energy. The various stimuli to which explosives respond and the manners of their responses in producing explosions provide a convenient basis for their classification. Alternatively, classifications based on chemical composition, particularly on the presence of the active nitrogenated (NO, NH, C-N etc.) or peroxide (O-O) group, are utilized.

Although the CB threats bear a strong impact on the media and impression on the minds of the population, the most preferred terrorists' tool still remains the use of explosive weapons, mainly because these are low-cost, available everywhere and relatively easy to handle. In the START database [6] bombing attacks account for about 49% of the terroristic actions perpetrated worldwide between January 1st, 1970, and December 31st, 2011, see Figure 1. The figure clearly depicts the problems come out after 9/11 event, which triggered an escalation of explosive attacks.

The majority of explosives are characterized by a very low vapor pressure, and even high sensitivity gas phase trace detectors cannot react to their presence. The first technology challenge for Security has been recognized in fast and reliable trace detection of explosives at *elementi o l'individuazione di gruppi funzionali, ad esempio, tramite la tecnica LIBS [13] nel primo caso e quella Raman nel secondo [14], sembra attraente per la possibilità di rilevamento remoto automatico e il monitoraggio a distanza, evitando qualunque problema dovuto alla possibile stanchezza di operatori umani o animali.*

In ogni caso la tecnologia progredisce e i terroristi sostituiscono gli esplosivi commerciali con gli IED, costruiti con esplosivi non disponibili in commercio, il più delle volte preparati in loco partendo da sostanze chimiche innocue. La definizione di uno IED concordata internazionalmente è la seguente: "Un qualunque dispositivo fabbricato in modo improvvisato che incorpora esplosivi o sostanze chimiche distruttive, letali, nocive, pirotecniche o incendiarie, progettato per distruggere, sfigurare, distrarre od ostacolare" [15].

Le informazioni incontrollate disseminate nel web e la presenza simultanea di persone altamente formate e laureate consente a un grande numero di individui di preparare e costruire IED contenenti esplosivi improvvisati (IE). Gli IE possono essere fabbricati in casa, con prodotti che possono essere acquistati senza alcuna autorizzazione specifica (ad es., nitrato di ammonio, pepe nero, perossido di idrogeno e altre sostanza chimiche). Tali sostanze sono comunemente definite come precursori di esplosivi. Ne consegue che la sfida tecnologica diventa il rilevamento di possibili precursori di esplosivi in luoghi imprevisti (ad es., una gran quantità di fertilizzanti nel garage di un appartamento di città) [5].

Il 22 luglio 2011 Anders Behring Breivik, di nazionalità norvegese, uccise 8 persone facendo esplodere un'autobomba (un VBIED, "dispositivo esplosivo improvvisato incorporato in un autoveicolo") nel quartiere governativo di Oslo (Norvegia). Il caso Breivik illustra che i precursori chimici di esplosivi sono facilmente ottenibili da chiunque sia in grado di inventare una ragione plausibile per procurarseli.

La Comunità Europea ha recentemente limitato la vendita sul mercato di precursori di esplosivi con il regolamento n. 98/2013 [16], nel quale sono elencate le sostanze che non saranno più rese disponibili al pubblico in generale, né da sole né miscelate, o sostanze che le includano, tranne nel caso in cui la concentrazione sia uguale o inferiore ai valori limite prefissati. Vi sono inoltre riportate le sostanze, da sole o miscelate, o contenute in composti che potrebbero indurre a transazioni sospette relative alla

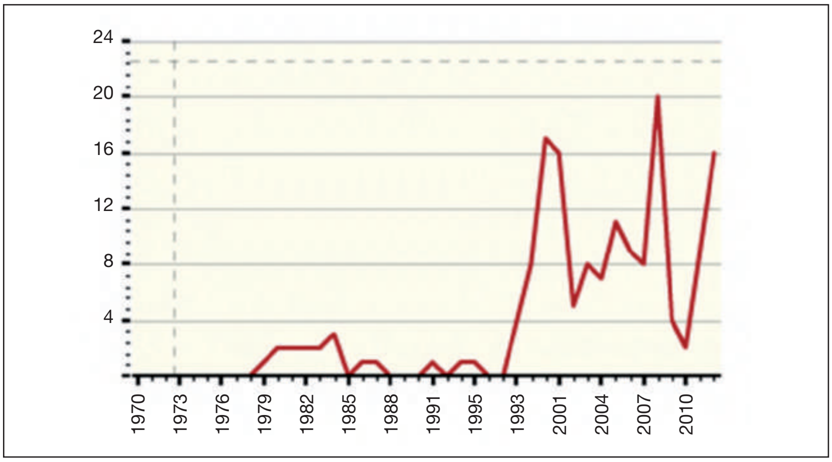


FIGURE 1 Worldwide explosives incidence from 1970 to 2010 year
Incidenza degli attacchi terroristici mediante esplosivi nel mondo dal 1970 al 2010
Source: [6]

transit points (gates in crowded areas) in order to replace the only sensitive and selective enough natural gas detector: the dog nose. Alternative spectroscopic detection of elemental composition or identification of functional groups, e.g. by LIBS [13] in the first case and by Raman in the second [14], appear appealing because of the chance of automatic remote detection and stand-off monitoring, without any problems related to the possible tiredness of human or animal operators.

Anyhow, technology is in progress and bombs made with commercial explosive are being replaced by terrorist with IEDs, where non-commercial explosives are utilized, most of the time produced in situ starting from harmless chemicals. The definition internationally agreed of an IED is the following: "Any device that is fabricated in an improvised manner, incorporating explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals, designed to destroy, disfigure, distract or harass" [15].

The uncontrolled information disseminated in the web and the simultaneous presence of highly trained and graduate personnel enables a large number of people to prepare and build IEDs containing Improvised Explosives (IE). IE can be realized at home, using products that can be bought without any specific authorization (e.g., ammonium nitrate, black pepper, hydrogen peroxide, and other chemical substances). These substances are commonly referred as explosive precursors. Hence, the technology challenge becomes the detection of possible explosive precursors at unexpected locations (e.g., large quantity of fertilizers in the garage of a city flat) [5].

compravendita e all'uso di precursori di esplosivi.

Il panorama degli attacchi terroristici con armi CBRNe si complica maggiormente con il concetto di "bomba sporca", che richiede un'ulteriore spiegazione. Una bomba sporca è un'arma radiologica ipotetica che combina materiale radioattivo con esplosivi convenzionali. Lo scopo di tale arma è di contaminare l'area circostante il cosiddetto "agente di dispersione" o '"esplosione convenzionale" con materiale radioattivo, fungendo primariamente da dispositivo per il divieto di accesso dei civili a una data area. L'uso di questo tipo di bomba sporca, basata sul Cesio-137, è stato rivendicato dai ribelli ceceni nei due attacchi falliti del 1995 a Mosca e del 1998 nei pressi di Grozny [17].

Tuttavia, è improbabile che una bomba sporca causi molte vittime da esposizione a radiazioni. Il suo scopo è presumibilmente quello di creare danni psicologici più che fisici, facendo leva sull'ignoranza e innescando meccanismi di panico e terrore di massa. Inoltre l'isolamento e la decontaminazione di migliaia di vittime, nonché la decontaminazione dell'area colpita potrebbero richiedere tempi e costi notevoli, rendendo tale area parzialmente inutilizzabile e causando pesanti danni economici. Per tale ragione oggi l'individuazione a distanza rapida e affidabile di bombe sporche rappresenta una importante sfida tecnologica.

Ricerca e sviluppo tecnologico per la security

Dal PASR-6PQ fino a Horizon 2020 tramite il 7PQ – Il panorama europeo

Il bisogno di un maggiore sforzo della ricerca europea per la security ha acquisito maggiore importanza dal 2002 al 2007, durante il Sesto Programma Quadro (6PQ). Attenzione è stata dedicata fin dall'inizio a bilanciare tale sforzo, affiancando i miglioramenti nelle forme di controllo con il rispetto della privacy e della libertà individuale. Bandi di progetto sono stati dedicati agli aspetti relativi alla security, in particolare allo spazio e all'aeronautica, nonché all'ICT. Inoltre, nello stesso periodo (2004-2006) è stata lanciata l'azione dedicata PASR (Preparatory Action for Security Research), che ha finanziato la realizzazione di progetti pilota. La lista delle misure di security nel 6PQ e nel PASR è disponibile in [18].

Nel frattempo, due commissioni (ESRIF - European Security Research and Innovation Forum, and ESRAB - European Security Research Advi-

On July 22nd, 2011, the Norwegian national Anders Behring Breivik killed 8 people through the explosion of a car bomb (a "vehicle-borne improvised explosive device", VBIED) in the government quarter of Oslo (Norway). The Breivik case illustrates that precursor chemicals are easily obtainable for anyone capable of inventing a plausible reason to procure them.

The EC has recently limited the market sale of explosive precursors with the 98/2013 regulation [16]. Substances which shall not be made available to members of the general public on their own, or in mixtures, or substances including them, except if the concentration is equal to or lower than the limit values set out, are listed. Furthermore, also substances on their own, or in mixtures, or in substances for which suspicious transactions referring to the marketing and use of explosives precursors are reported.

The terroristic attack panorama, based on CBRNe weapons, is further complicated by the concept of "dirty bomb", which requires an additional explanation. A dirty bomb is a speculative radiological weapon that combines radioactive material with conventional explosives. The purpose of the weapon is to contaminate the area around the "dispersal agent"/"conventional explosion" with radioactive material, serving primarily as an area denial device against civilians. The use of such a type of dirty bomb (based on Caesium-137) has been claimed *sory Board), composte da specialisti e strateghi altamente qualificati, hanno stilato le linee strategiche per la ricerca europea sulla security, suggerendo i principi e i meccanismi per la loro adozione all'interno del Settimo Programma Quadro (7PQ) per la Ricerca della Commissione Europea.*

Nel 7PQ è stata aggiunta una priorità tematica (tema 10) sulla Security, quale specifico programma di cooperazione, ponendo l'attenzione sulle quattro missioni della Security suggerite dall'ESRAB [19]:

- *security dei cittadini;*
- *security delle infrastrutture e dei servizi pubblici;*
- *sorveglianza intelligente e security di confine;*
- *ristabilire condizioni di security e sicurezza personale in caso di crisi.*

Inoltre, sono state considerate tre attività trasversali: Integrazione, interconnettività e interoperabilità dei sistemi di security; Security e società; Coordinamento e strutturazione della ricerca sulla security.

Oggi, i temi relativi alla security sono ritenuti della massima importanza nei programmi di cooperazione internazionale. L'argomento relativo alla protezione dei cittadini è incluso nel programma di ricerca europeo Horizon 2020 (H2020). In particolare, appartiene ad uno dei tre maggiori pilastri, l'unico relativo alla società sicura, finalizzato alla protezione della libertà e della security dell'Europa e dei suoi cittadini.

La sfida sulla security posta da H2020 consiste nell'intraprendere tutte le attività di ricerca e di innovazione necessarie alla protezione dei cittadini, della società e dell'economia, nonché di servizi e infrastrutture, della prosperità, della stabilità politica e del benessere. Secondo la dichiarazione ufficiale della Comunità Europea riportata in [20], gli obiettivi primari della sfida per una società sicura sono:

- *migliorare la resistenza della nostra società contro le catastrofi naturali e quelle causate dall'uomo;*
- *combattere il crimine e il terrorismo;*
- *migliorare la security ai confini;*
- *fornire una migliore security telematica.*

Altri promotori internazionali della security

L'Agenzia Europea per la Difesa (AED) è il luogo di riferimento per la cooperazione per la difesa europea sin dal 2004, anno della sua fondazione. Tra i suoi impegni istituzionali, l'AED

by Chechen rebels in two failed attacks in 1995 and 1998, the first in Moscow and the second near Grozny [17].

However a dirty bomb is unlikely to cause many deaths by radiation exposure. Its purpose would presumably be to create psychological, not physical, harm through ignorance, mass panic, and terror. Additionally, containment and decontamination of thousands of victims, as well as decontamination of the affected area might require considerable time and expense, rendering areas partly unusable and causing economic damage. For this reason, nowadays fast and reliable remote identification of dirty bombs is a significant technological challenge.

RTD for security

From PASR-FP6 through F7 to Horizon 2020 – The European panorama

The needs to increase European research effort on security became significant during the 6th Framework Programme (FP6) in 2002-2007 period. Attention was paid to balance it, which implied enhanced forms of control, with the respect of privacy and individual freedom. Calls for projects were dedicated to aspects concerning security, especially for aeronautic and space, and for ICT. Additionally, in the same period (2004-2006) the dedicated PASR (Preparatory Action for Security Research) action was launched, funding pilot projects. A review of security measures in FP6 and PASR can be found in [18].

Meanwhile two commissions (ESRIF - European Security Research and Innovation Forum and ESRAB - European Security Research Advisory Board), composed by highly qualified specialists and strategists, have drawn the strategic lines for European security research and advised on the principles and mechanism for its implementation within the Commission's 7th Framework Programme (FP7) for Research.

In FP7 a thematic priority (theme 10) on Security was added, as a specific cooperation programme. The focus was set on the four Security missions suggested by ESRAB [19]:

- Security of citizens,
- Security of infrastructure and utilities,
- Intelligent surveillance and border security,
- Restoring security and safety in case of crisis.

Furthermore three cross cutting activities were considered: Security systems integration, interconnectivity and interoperability, Security and Society, Security Research coordination and structuring.

Nowadays, the themes related to security are of utmost importance in international cooperation programs. The topic, relevant to Citizen protection, is included in Horizon 2020 (H2020), the current European research programme. In particular, it belongs to one of the three major pillars, the one relevant to Secure society, aimed at protecting freedom and security of Europe and its citizens.

porta avanti anche progetti di ricerca e sviluppo tecnologico, iniziative a supporto dell'industria europea della difesa e un metodo innovativo di duplice utilizzo. Il Ministero della Difesa dei rispettivi paesi membri assicura il proprio supporto ai nuovi progetti.

Il programma Science for Peace and Security (SPS), originariamente nato come programma scientifico della NATO negli anni Cinquanta, offre finanziamenti per attività di progetti di collaborazione, workshop e formazione, che coinvolgono scienziati provenienti dai paesi membri della NATO e dai paesi partner. L'SPS è uno strumento politico per migliorare la cooperazione e il dialogo con tutti i partner e costituisce una palestra interessante per i giovani ricercatori, che collaborano anche con paesi extra NATO.

Parallelamente, varie lobby europee sono attive nel panorama della security, promuovendo i bisogni e le nuove aspettative degli operatori o dei portatori di interesse che intendono avere un dialogo specifico con la CE. Tra queste, l'AeroSpace and Defense Industries Association of Europe rappresenta le maggiori industrie europee nel campo dell'aeronautica, spazio, difesa e security. Diversamente, l'Integrated Mission Group for Security (IMG-S) è un forum pubblico che riunisce gli esperti di tecnologie provenienti da industria, PMI, Organizzazioni di Ricerca e Sviluppo e dal mondo universitario. IMG-S fornisce il proprio supporto alla Commissione Europea e agli Stati Membri nella costruzione di capacità tecnologiche europee di classe mondiale.

Lo scenario italiano

Vari paesi europei come, per citarne alcuni, Germania, Gran Bretagna, Olanda, Svezia, hanno incluso nel proprio programma nazionale dedicato il supporto alla ricerca sulla security, in maniera analoga, ma non speculare, ai Programmi Quadro europei. Al contrario, in Italia non è disponibile alcuna opportunità di finanziamento, malgrado la security per la difesa nazionale sia citata nel Programma di Ricerca Nazionale 2011-2013.

A livello nazionale, la piattaforma italiana per la security SERIT (Security Research in Italy) è un'iniziativa congiunta lanciata da CNR e Finmeccanica, che riunisce industrie italiane (grandi industrie e PMI), università, centri di ricerca e utenti finali. L'obiettivo è lo stesso del suo gemello IMG-S, ma con un legame più forte con le autorità nazionali.

The challenge on security afforded by H2020 is about undertaking research and innovation activities needed to protect our citizens, society and economy as well as our infrastructures and services, our prosperity, political stability and wellbeing. According to the official European Community statement reported in [20], the primary aims of the Secure Societies Challenge are:

- *to enhance the resilience of our society against natural and man-made disasters;*
- *to fight crime and terrorism;*
- *to improve border security;*
- *and to provide enhanced cyber-security.*

Other international security promoters

The European Defense Agency (EDA) is the place to go for European defense cooperation since its foundation in 2004. EDA, among its institutional commitments, conducts also RTD projects, works on initiatives in support of the European defense industry, and advances an innovative dual-use approach. The Ministry of Defense of the respective member states assures the support of the new projects.

The Science for Peace and Security Programme (SPS) originally founded as the NATO Science Programme in the 1950s, offers grants for collaboration projects, workshops and training involving scientists from NATO member states and partner countries. SPS is a policy tool for enhancing cooperation and dialogue with all partners, and is an interesting palaestra for young researchers to collaborate also with extra NATO countries.

In parallel, different European lobby organizations are active in the Security panorama, fostering the needs and new expectations from the operators or stakeholders that intend to have a specialized dialogue with the EC. Among them the AeroSpace and Defense Industries Association of Europe represents the major aeronautics, space, defense and security industries in Europe. Conversely, the Integrated Mission Group for Security (IMG-S) is an open forum bringing together technology experts from Industry, SMEs, Research and Technology Organizations (RTOs) and Academia. IMG-S aims to support the European Commission and its Member States to build world-class European technological capabilities.

The Italian background

Different European countries, Germany, Great Britain, Holland, Sweden, just to mention a few, have included in their own dedicated national program the support to Security research, analogous but not mirrored to the EU Framework Programs. Conversely, in Italy no specific funding opportunities are available, although the Homeland Security is indicated in the National Research Program 2011-2013.

Scenari di riferimento

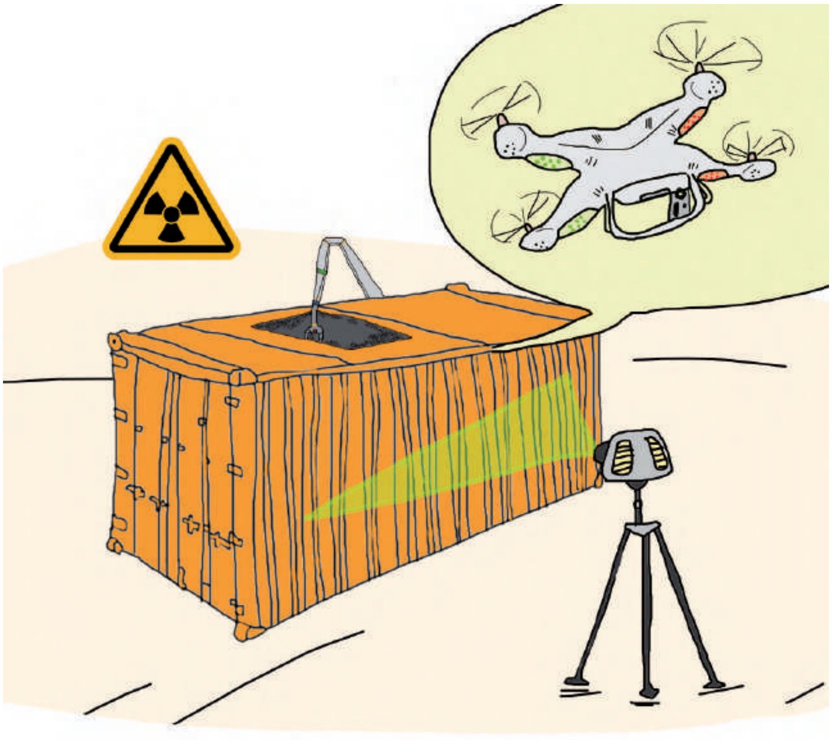
Security per il trasporto di massa e la gestione delle folle

La mobilità globale è una conquista importante della società industriale moderna, che comporta una rete complessa di infrastrutture, nelle quali il flusso di gente, informazioni e merci è stato molto semplificato. Le criticità emergono là dove le minacce attuali a cui è sottoposta la società sono numerose e complesse. In siti molto affollati come, ad esempio, i punti di scambio per il trasporto, le operazioni vengono spesso eseguite al limite della capacità delle infrastrutture, rendendole in tal modo maggiormente vulnerabili a eventuali attacchi.

La società, viceversa, non è chiamata a far fronte a una singola minaccia o pericolo, ma a numerose prove, quali terrorismo, crimine organizzato, instabilità regionale e calamità naturali, che esigono altrettante azioni tecnologiche e non tecnologiche di natura preventiva e contromisure. Ne consegue che la tecnologia e le metodologie utilizzate per identificare la varietà delle minacce devono essere rapide e versatili, capaci di rilevare quantità massicce o tracce di agenti CBRNe e armi nascoste, senza causare disordine o ritardi eccessivi.

Lo sviluppo di strumenti multiuso per il rilevamento rapido di immagini con il riconoscimento automatico della minaccia è l'obiettivo finale adatto a un comune scenario di varchi per il trasporto di massa e, più in generale, a punti di controllo. Nel primo caso, varchi attivi o passivi dovrebbero essere utilizzati per passeggeri e bagagli a mano; nel secondo, i portali dovrebbero consentire lo screening del contenuto di valigie di varie dimensioni, da quelle personali ai container che viaggiano su grandi aerei, navi e treni merci. I requisiti di protezione della sicurezza personale e della privacy sono molto diversi nei due casi, con pesanti restrizioni per l'uso di radiazioni ionizzanti e potenzialmente nocive (persino nella regione microonde - THz) su esseri umani, tuttavia la rapidità è fondamentale in entrambi. Oltre alle armi e agli esplosivi, i materiali da identificare possono essere diversi, inclusi, ad esempio, i precursori di IED sui passeggeri o i radionuclidi nascosti nelle merci [21].

Etichettare persone e oggetti sospetti durante il percorso di imbarco sarebbe una procedura appropriata che consentirebbe di eseguire le successive misure di conferma utilizzando



At the national level, the Italian Security platform SERIT (Security Research in Italy) is a joint initiative launched by CNR and Finmeccanica, bringing together Italian industries (both large industries and SMEs), academia, research centers and end-users. Its final aim is the same as that of the twin IMG-S but with a stronger connection with the national authorities.

Reference scenarios

Mass transport security and crowd management

Global mobility is a significant achievement of the modern industrial society involving a complex network of infrastructures, where people, information, and goods can easily flow. Critical points emerge where current threats facing society are numerous and complex. In very crowded sites, such as transport hubs, operations often proceed at the limit of the infrastructure capability, thus increasing its vulnerability to attacks. Conversely, society is not called to face a single threat or hazard, but a variety of challenges such as terrorism, organized crime, regional instability and natural disasters, that demand a corresponding variety of non-technological and technological actions, of a preventive *tecnologie alternative, riducendo drasticamente il numero di falsi positivi. La lunghezza del percorso da seguire durante le suddette procedure e i tempi richiesti svolgono un ruolo significativo nella selezione delle diverse tecnologie per i controlli successivi. A questo riguardo, lo scenario del trasporto urbano è di gran lunga più severo di quello relativo al traffico aereo.*

Per ottenere la massima attenzione dell'opinione pubblica, un gruppo terroristico tende a colpire aree affollate, dove la quantità di agenti disturbatori presenti potrebbe consentire di raggiungere la massima distruzione. In caso di panico, proprio il comportamento della folla potrebbe causare ulteriori vittime, anche in conseguenza di una minaccia di minima entità.

La gestione delle folle richiede che siano considerati tutti gli elementi di un evento, partendo dalla sua tipologia (spettacolo circense o sportivo o teatrale, concerto, rally, parata, ecc.), le caratteristiche della struttura e suoi accessi, le comunicazioni disponibili, la dimensione e il comportamento della folla, le possibilità di un suo controllo anche nello smaltimento delle code. Come accade per ogni tipo di gestione, occorre tenere conto della pianificazione, l'organizzazione, il reclutamento di personale la direzione e la valutazione. Particolarmente importanti per la gestione delle folle sono la definizione dei ruoli delle parti coinvolte in un evento, la qualità delle risorse di intelligence avanzata e l'efficacia del processo di pianificazione.

Lo sviluppo tecnologico nella gestione delle folle è mirato sia alle misure preventive, sia agli interventi. Lo screening delle folle mediante il rilevamento automatico di comportamento sospetto (insolito), che fa scattare i sensori per minacce specifiche su un target selezionato (potenziali terroristi), appartiene al primo gruppo, mentre la pronta attivazione automatica di vie di fuga, assistita da dispositivi autonomi non gestiti da operatori umani e tramite strumenti di ICT, è un esempio del secondo gruppo.

Sistemi di reti di rilevamento e accettazione etica

Gli scenari fin qui presentati sono molto complessi a causa della loro grande variabilità e di minacce rilevanti che, nella maggior parte dei casi, sono quasi imprevedibili. Diverse tecniche di rilevamento, che nel caso dei sensori

nature as well as counter measures. Consequently the technology and the methodologies used to identify the variety of threats must be fast and versatile - capable of dealing with the detection of hidden bulk and trace of CBRNe agents and concealed weapons, without causing excessive disruption or delay.

The development of multipurpose instrumentation for fast imaging with automatic recognition of the threat is the final objective suitable for a common scenario at mass transport gates, and more generally at custom controls. In the former case, active or passive gates should be utilized on people and their hand luggage, in the latter portals should permit the screening of the content of differently-sized luggage, from personal suit cases to containers travelling on large cargos planes, ships and trains. Safety and privacy requirements are largely different in the two cases, with heavy restrictions to the use of ionizing and potentially harmful radiation (even in the microwave - THz region), however speed is crucial in both cases. Apart from weapons and explosives, the target materials to be detected might be different, including for instance IED precursors on passengers or radionuclides hidden with goods [21].

Labelling suspect persons and items during a loading path is a successful procedure that might permit to perform successive confirmation measurements by alternative technologies in order to drastically reduce the number of false positives. The length of the path to be followed during the boarding procedures and the time required do play a significant role in selecting different technologies for successive checks. To this respect the scenario for urban transport is by far more stringent than that relevant to airport traffic.

With the aim of maximizing the attention from public opinion, a terroristic group tends to strike in a crowded area, where the same quantity of disruptive agents could allow to achieve the most destruction. In case of panic the crowd behavior itself can cause additional loss of human lives, even as a consequence of a very minor threat.

Crowd management must take all the elements of an event into account, especially the type of event (circus, sporting, theatrical, concert, rally, parade, etc.), characteristics of the facility, size and demeanor of the crowd, methods of entrance, communications, crowd control, and queueing. As in all management, it must include planning, organizing, staffing, directing and evaluating. Particularly critical to crowd management is defining the roles of the parties involved in an event, the quality of the advance intelligence, and the effectiveness of the planning process.

Technologic development in crowd management is addressed to both preventive measures and interventions. Crowd screening with automatic detection of suspect (unusual) behavior triggering sensors for specific threats on a selected target (potential terrorists) belongs to the first group, while prompt automatic activation of escape route *elettro-ottici coprono l'intero spettro elettromagnetico, possono essere utilizzate per fornire informazioni rapide ed efficaci sulla eventuale presenza di sostanze sospette.*

Il metodo emergente per far fronte alla security in tutti i tipi di scenario consiste nell'integrare le informazioni (video, chimiche, fisiche), raccolte da una rete di vari sensori e sistemi di consapevolezza ambientale, e convogliarle in un Centro di Comando e Controllo supportato dalle tecnologie Expert System. La rete deve garantire la confidenzialità dei dati ed essere predisposta per accogliere la futura integrazione di nuovi dispositivi, che consenta la realizzazione di una cosiddetta 'architettura aperta'.

Attualmente, il modello di security adottato negli aeroporti è forse l'esempio migliore per l'intenso lavoro normativo eseguito dall'International Civil Aviation Organization, dove le necessità emergenti vengono discusse e le contromisure individuate e proposte mediante norme che ne definiscono le caratteristiche logistiche e tecniche. Ovviamente i diversi scenari andranno modificati in modo che in futuro possano essere progettati con proprie infrastrutture di security già incorporate. È prevedibile che tecnologie a distanza, basate su radiazioni non-ionizzanti, svolgeranno un ruolo sempre più importante senza però sostituire completamente il rilevamento puntuale, necessario per la conferma locale, i successivi interventi delle autorità competenti e l'uso in campo forense.

Tutte queste tecnologie di screening non riscuotono l'accettazione immediata da parte della società civile, a causa dell'invasione della privacy che potrebbe limitare la libertà individuale. Ne consegue necessariamente che, per un risultato soddisfacente occorre trovare un equilibrio tra l'applicazione di misure efficaci per migliorare la security e il rispetto dei diritti civili.

(traduzione di Carla Costigliola)

assisted by unmanned autonomous vehicles and by available ICT tools is an example of the second one.

Networked Detection Systems and ethical acceptance

The scenarios presented above are very complex having a large variability, and relevant threats are in most cases almost unpredictable. Numerous different detection techniques, covering all the electromagnetic spectrum in case of electro-optical sensors, can be utilized to supply rapid and effective information on the presence of suspicious substances.

The emerging approach to face security in all the scenarios is to integrate the information collected from a network of various sensors and systems of environmental awareness (video, chemical, physical), and to merge it in a Command and Control center supported by Expert System technologies. The network has to ensure the confidentiality of the data and to be open to the future integration of new devices, in a so-called open architecture.

Presently, the security model adopted in the airports is perhaps the best example due to the intense regulation work performed by International Civil Aviation Organization, where the emerging needs are discussed and the countermeasures regulated in both logistic and technical characteristics. Obvious modifications to the different scenarios have to be adopted, so that in the future they already have to be designed with their own security infrastructures embedded. It is predictable that stand-off technologies based on non-ionizing radiations will play an increasing role, without completely replacing the point-detection necessary for local confirmation, next authorities intervention and forensic use.

These screening technologies are not so immediately acceptable by the civil society, due to the privacy invasion that can affect the individual freedom. A balance between implementing effective measures to improve security and respecting civil rights is mandatory to obtain a satisfactory result.

Roberta Fantoni
ENEA, Technical Unit for the Development of Applications of Radiation

Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation - Diagnostics and Laser Metrology Laboratory

references & notes

[1] M. Minichino et al, Quality of service of an electrical grid under cyber attacks on its Supervisor Control and Data Acquisition System (this issue).

[2] F. Padoani, A. Rizzo, Developing the human dimension of security by means of centres of excellence (this issue).

[3] A. Malizia et al, Building a Chemical-Biological-Radiological-Nuclear, Eplosive events tech advisor and first responders team to support top decision makers during the emergencies (this issue).

[4] V. Rosato et al, Decision support system aimed at improving the "physical protection" of critical infrastructures against natural events (this issue).

[5] L. Fiorani et al, Lidar/DIAL detection of explosive precursors by OPO/OPA laser systems (this issue).

[6] National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database, http://www.start.umd.edu/gtd [Accessed 3 November 2013].

[7] D. J. Dire, 2013, CBRNE - Biological Warfare Agents, Medscape, New York, NY.

[8] United Nations - Security Council, 2006, Twenty-sixth quarterly report on the activities of the United Nations Monitoring, Verification and Inspection Commission in accordance with paragraph 12 of Security Council resolution 1284 (1999), United Nations, New York, NY. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1284(1999)

[9] J. Du, 2002, Bioterrorism: How Has It Been Used? What Can It Do? How Prepared Are We? UCLA, Los Angeles, CA– http://www1.international.ucla.edu/article.asp?parentid=1352

[10] Federal Bureau of Investigation, Famous Cases and Criminals: Amerithrax or Anthrax Investigation, FBI, [Online]. Available: http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax [Accessed 3 November 2013].

[11] A. Lai et al, Innovative devices for biohazards and food contaminants (this issue)

[12] H. Murakami, 2003, Underground. Racconto a più voci dell'attentato alla metropolitana di Tokyo, Einaudi, ISBN 978-88-06-16521-5.

[13] V. Lazic et al, 2011, "Detection of explosives in traces by laser induced breakdown spectroscopy: Differences from organic interferents and conditions for a correct classification", Spectrochim. Acta Part B, 66 ,644–655.

[14] A. Palucci et al, Raman spectroscopy for the detection of trace amounts of energetic materials for counterterrorism issues (this issue).

[15] NATO STANAG AAP6-6+Interagency Intelligence Committee on Terrorism – From Enhancing the security of explosives – Report of the explosive security experts task force, Brussels, 28 June 2007, http://nso.nato.int/nso/

[16] Regulation (EU) No 98/2013 of the European Parliament and of The Council of 15 January 2013 on the marketing and use of explosives precursors. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:039:0001:0011:EN:PDF

[17] J. Bale, 2004, The Chechen resistance and radiological terrorism, Global Security Newswire, Article, April 1st 2004 - http://www.nti.org/analysis/articles/chechen-resistance-radiological-terror

[18] D. Bigo, J. Jeandesboz, 2008, DG Internal Policies of the Union, briefing note PE 393.289 (May 2008), http://edz.bib.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf

[19] European Security Advisory Board (ESRAB), Meeting the Challenge: the European Security Research Agenda, Office for Official Publications of the European Communities, Luxembourg, 2006 - http://cordis.europa.eu/fp7/security/about-security_en.html

[20] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

[21] Di Lazzaro et al, Marking and tracking radioactive materials: a possible Hi-TECH solution (this issue).

Le nuove tecnologie e le attività di polizia: security e problematiche forensi

Nuove tecnologie, capaci di rilevare la presenza di esplosivi, sono state sviluppate a seguito dell'evoluzione della minaccia di attacchi terroristici nei confronti di possibili bersagli, quali aeroporti e altri mezzi pubblici di trasporto. La security e le problematiche forensi necessitano una valutazione fin dal primo stadio della ricerca, affinché le attività di pubblica sicurezza e di polizia giudiziaria siano supportate in maniera efficace. La capacità analitica di ciascun rilevatore può essere misurata seguendo un approccio probabilistico, basato sui risultati (veri positivi, veri negativi, falsi positivi e falsi negativi) ottenuti in una serie di test su campioni noti. Nelle attività relative alla security, quali i punti di controllo e screening dei passeggeri negli aeroporti, è importantissimo evitare falsi negativi, che comporterebbero l'imbarco di un oggetto proibito. I falsi positivi possono essere accettati, anche se dilatano il tempo necessario per lo screening dei passeggeri e dei loro bagagli. In progetti mirati a individuare una 'fabbrica di bombe' criminale è fondamentale evitare falsi positivi in modo da risparmiare ai cittadini una inutile invasione della propria privacy. Se infine si considera il mondo forense tradizionale, quando si riportano dati chimici come prove in un processo, l'incertezza deve essere ridotta al minimo, in quanto la Corte deve essere messa in grado di stabilire la verità oltre ogni ragionevole dubbio.

New technologies and police activities: Security and forensic issues

The development of new technologies able to detect explosives has followed the evolution of the threat of terrorist attacks to possible targets, such as airports and other public transport. The security and forensic issues need to be evaluated in the early research stage to effectively support police activities. The analytical capability of any detector can be measured by following a probabilistic approach, based on the results (true positives, true negatives, false positives and false negatives) obtained in a set of tests on known samples. In security activities, such as at passenger screening checkpoints in airports, it is very important to avoid false negatives, resulting in a forbidden item being boarded. False positive results can be accepted, but they increase the time needed for screening passengers and their luggage. In projects aiming to spot a criminal "bomb factory" it is very important to avoid false positive results so as to spare citizens useless intrusion in their private lives. When considering the traditional forensic world, uncertainty must be minimised when reporting chemical information as evidence in the Court, since the Court needs to establish the truth beyond any reasonable doubt.

DOI: 10.12910/EAI2014-86

■ *F.S. Romolo, G.G. Vadalà*

■ Contact person: Francesco S. Romolo
francescosaverio.romolo@uniroma1.it

Introduction

The use of new technologies for police activities is a very interesting subject to discuss how research and development of new technological tools can help guarantee people the right to security with increased efficacy. A major threat is the criminal use of explosives by terrorists. New tools, aimed at detecting illegal activities in their early stages or trace of the explosive used after an attack, need to be conceived on a fitness-to-purpose basis. Security and forensic issues need to be evaluated in the early stage of the research and development process so as to avoid that new tools do not properly fit with the police needs.

Explosives, whether compounds or mixtures, are substances, "which are in a metastable state and are capable, for this reason, of undergoing a rapid chemical reaction without the participation of external reactants such as atmospheric oxygen" [1].

Explosives can be divided into six groups from a chemical point of view: nitro-compounds (dinitrotoluene, trinitrotoluene), nitric esters (nitroglycerine, nitrocellulose, pentrite), nitramines (RDX, HMX), derivatives of chloric and perchloric acids, and a last group of various compounds capable of producing an explosion, such as fulminates or peroxides. The peroxide-based explosives such as triacetone triperoxide (TATP) and hexamethylene triperoxide diamine (HMTD), belonging to the last group of various compounds, have been recently involved in terrorist attacks [2-5].

There are still restrictions for passengers on carrying liquids, aerosols and gels (LAGs) aboard, introduced in 2006 following a foiled plot to detonate homemade liquid explosives aimed at blowing up several aircrafts during the flight from London-Heathrow Airport [6].

The role of chemistry in this type of forensic studies is very important [7] and a preliminary discussion about the relationship between chemistry and forensic science will help to understand how new technologies can support the police dealing with security and forensic issues.

Chemistry and forensic science

In the XIX century the publications about the use of chemistry to help solve forensic problems dealt mainly with toxic substances and poisons. Naquet wrote about «Legal Chemistry», which «is applied to that branch of the science which has for its office the solution of problems proposed in the interest of Justice» [8]. Following the historical evolution in this field, it is possible to recognise that some fundamental issues, such as the meaning of legal or forensic chemistry, were never discussed and clarified. In 1981, Maehly and Stromberg [9] wrote about chemical criminalistics and admitted that «the definition of this discipline is still under discussion and varies from country to country». In the present paper we are going to talk about chemistry and forensic science, considering how technology can support the police forces in their activities to guarantee the security of citizens and during the criminal investigations.

Technology and security

On December 10th, 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights, where it is stated that «Everyone has the right to life, liberty and security of person» [10]. Prevention of crimes is a priority for all police forces all over the world. When dealing with threats to people and properties, the subjects in charge of security can decide to take an action such as to open correspondence or to stop the people getting on a plane, if the presence of an explosive charge is suspected.

Police forces and other subjects in charge of security are often helped by technological tools, developed to detect explosives, firearms and other dangerous items. In airports the design concept of passenger screening checkpoints is based on a multi-level approach with arch metal detectors and conventional *x*-ray equipment, followed by advanced metal, explosive and hazardous substance detectors, and state-of-the-art *x*-ray equipment. A complete manual physical search can be finally carried out whenever needed.

The most common systems for field screening of explosive traces to be used (see Figure 1) are ion mobility spectrometers (IMS) and chemiluminescence detectors [11, 12]. Ion Mobility Spectrometry (IMS) is a high sensitive analytical technique able to detect a wide range of chemical compounds (both organic and inorganic) at trace levels in gas phase or particulate.

FIGURE 1 Portable explosive detector used in criminal investigations in Italy. Courtesy of. G.G. Vadalà

Most of the IMS applications are in the military, security and forensic fields (chemical warfare agents, explosives and illicit drugs), mainly because analyses can be very fast and IMS instruments can be rugged enough to be field-portable and easy to use to enable non-scientific personnel to operate it under strictly controlled conditions. Another analytical system used for detection of explosives is EGIS®, originally based on high-speed gas chromatography, combined with a highly selective and sensitive chemiluminescence detector, able to screen carry-on baggage, checked baggage, vehicles. A key issue when detecting explosives is the vapour pressure of explosives [13].

Currently, trained dogs can be considered the best choice to detect explosives in the vapour phase since there are able to give positive results at lower concentrations compared to technology-based sensors [14]. However, the development of new technologies and devices is increasingly necessary, especially because dogs can only work for a short period of time before being fatigued.

The analytical capability of a detector can be measured following a probabilistic approach, based on the results (true positives, true negatives, false positives and false negatives) obtained in a set of tests on known samples. For example it is easy to recognise that metal detectors have a high rate of "false alarms", meaning that most of the alarms do not correspond to firearms or other dangerous metal items. These results can be used to calculate the false alarm rate and the probabilistic sensitivity and specificity of the technique. The probabilistic sensitivity is the probability to have a positive result, given the presence of the searched substance. The probabilistic specificity is the probability to have a negative result, given the absence of the searched substance. Whenever an alarm is given by a detector, the following decision/action depends mainly on the legal framework, the parameters determining the analytical capability of the detector and the time limit for the decision/action. In an airport, an example of false negative result is a terrorist boarding on a plane with an explosive charge. Passenger screening checkpoints need to avoid false negative results, but it is also necessary to consider that the time required for screening passengers and their luggage has to be limited. All the people giving false positive results suffer additional time spent for a complete manual physical search. Any technology for security needs to give evidence of clinical, social, and ethical acceptability, too [15]. A good example of study of the effects on health of security technologies is in the document of the EU Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) about scanners for passenger screening based on x-ray technology [16].

There is another aspect of the relationship between technology and security to be discussed. «Police officers who respond to a potential dangerous event must do so within the limitations of their training, support network and equipment. Personal safety is a primary concern» [17]. When specialists arrive on the scene of a (possible) crime, spot tests or chemical detectors can play a critical role if explosive substances are present. The best implemented strategy is based on chemical information (e.g., adopting self-protection measures, setting up an incident command centre, throwing a cordon...). In these situations not only probabilistic sensitivity and specificity, but also the limited time that can be waited before taking any decision must be considered. A detector with very good detecting capability can be useless if the analysis time is too long. The spot tests can be very useful for bulk detection. An example are the field tests for TNT based on the formation of coloured Meisenheimer and Janowsky anions in alkaline acetone or methanol. For more sensitive approaches there are procedures based on fluorescence emission or on optical chemosensing, yet the use of biosensors generally results in procedures having the best selectivity [18-21].

Spectroscopic approaches such as micro-Raman spectroscopy are capable of very sensitive detection, enabling to detect the amount of explosive obtained from a single fingerprint [22], or permit Standoff Detection, allowing a particularly safe approach to the chemical analysis of explosives [23], also permitting the analysis of explosives enclosed in containers [24].

For any incident involving dangerous materials, including explosives, it is important to avoid false negatives, resulting in possible unsafe behaviours in the presence of dangerous materials.

Research projects looking for new technologies able to detect and locate the illicit production of explosives in an urban environment have been carried out in the latest years and some of them are ongoing. FOI in 2012 exhibited the LOTUS project bomb-sniffer sensor, "the Raman system for the remote detection of traces of explosives, which is used under the EMPHASIS and HYPERION projects, as well as a biodetector based on honey bees for the detection of explosives, used under the PREVAIL project" [25].

In projects involving chemical sensors there are several possible operational advantages, e.g.:

1) real-time determination of the concentrations of specific sample constituents;
2) little to no power consumption;
3) operation without consumables and frequent maintenance;
4) unobtrusive sensing;
5) deployment in multiple locations forming distributed sensor networks" [26].

The most important requirements are always the sensitivity and the selectivity. When the aim of the network is to spot a criminal "bomb factory", it is very important to avoid false positive results so as to spare citizens useless intrusion in their private lives.

A project of this type is BONAS (BOmb factory detection by Networks of Advanced Sensors), aiming to design, develop and test a novel wireless sensor network for increasing citizen protection and homeland security against terrorist attacks, especially against the threat posed by Improvised Explosive Devices (IEDs) [27]. The sensor network will focus on the detection of traces of precursors used to produce IEDs. In this type of network approach, a key role is played by data fusion, considering that there are relatively few practical examples of data fusion in explosives detection and not many case studies [28].

Technology and forensic issues

The development of new methods for the analysis of explosives is of increasing importance not only for security issues but also for establishing criminal evidence [29]. There are two main types of forensic problems in casework: bulk analysis and trace analysis of residues. General comprehensive schemes for the analysis of post-explosion residues where first described in the 1970s. They can include the team approach for processing bomb-scene, visual examination of debris, sample preparation and analysis [30]. Analysis of traces on suspects or on their belongings are carried out with the same analytical techniques used for post-explosion residues but with different sampling approaches. Field tests on the crime scene «significantly enhance the productivity of the investigative/forensic science interface» [31]. The work of experts after the bombings occurred in Bali on 12th October, 2002 is a good example of the importance of having timely, albeit tentative analytical information at the crime scene [32]. The organic explosive trinitrotoluene (TNT) was detected using IMS at the scenes and confirmation was achieved by both gaschromatography (GC) with a chemiluminescence detector called Thermal Energy Analyser (TEA) and GC with Negative Chemical Ionisation Mass Spectrometry (NCI-MS).

Another example of how the detectors developed for airport security can be useful during criminal investigation is the use of EGIS® to make screening analyses during the investigation following the five bombings with explosive cars or vans, organised by Mafia, occurred in Italy in 1993 (three in Rome, one in Florence, and one in Milan). During the following years explosive detectors such as IMS or EGIS® were successfully used in the places were some explosive charges were prepared or hidden before the attacks. Results were later confirmed with other analyses [33] and reported to the Court. The term «confirmation» has gained widespread acceptance in analytical toxicology after appearing in the Mandatory Guidelines for Workplace Drug Testing in 1988. A confirmatory method provides full or complementary information, enabling to identify and, if needed, quantify the substance at the level of interest. Then, knowing which and how many analysis are required for identifying an explosive's trace is the main aspect in analytical chemistry, when applied to criminal investigations. If we want to give an unambiguous identification of a substance, necessary to report the chemical information as evidence in the Court, we must maximise the selectivity of the analytical procedure used. Using the probabilistic language it is possible to say that it is necessary to maximise the probability of the final analytical result supposing the presence of the compound of interest, and to minimise the probability of the analytical result given an alternative explanation. In some laboratories samples were analysed by gas chromatography and TEA three times, using three different columns. For others the minimum requirements for a positive identification is a separation technique combined with two detectors, based on different principles, or alternatively two separation techniques with one specific detection method [34]. The European Commission Decision of 12th August, 2002, implementing the Council Directive 96/23/EC concerning the performance of analytical methods and the interpretation of results, has become a reference document for any method in analytical chemistry having a forensic use [35]. According to this document, hyphenated techniques based on chromatography and mass spectrometry are the preferred methods to make confirmatory analysis, while methods based on chromatographic analysis without the use of spectrometric detection are not considered as suitable on their own for use as confirmatory methods. The European Council allows the use of a combination of independent techniques to confirm the identity of a substance. In this case a minimum number of identification points (IP) associated with each technique needs to be obtained. The Commission Decision includes performance criteria both regarding chromatographic separation and concerning the mass spectrometric analysis. The maximum number of identification points required in the Commission Decision is 4, corresponding to 4 ions in the Selected Ion Monitoring (SIM) or 2 fragments from the same precursor ion in tandem mass spectrometry. However, in order to qualify for the identification points required, a minimum of at least one ion ratio shall be measured and all relevant measured ion ratios shall meet some criteria.

Selectivity is the most important feature in validating an analytical procedure for forensic purposes, producing results to be reported as evidence in the Court, because of the need to establish the truth beyond any reasonable doubt. To explain the difference between a detection method and a confirmation method, it is possible to compare a fast and cheap method based on GC-MS to detect TATP [36] with a more expensive and time-consuming one based on HPLC-MS-MS [37]. The former is useful for security issues or to select forensic samples, but only the latter allows enough selectivity to avoid false positive and to report to the Court the chemical identification of TATP (the samples resulting positive after the GC method must be confirmed by the HPLC method).

Conclusions

When describing the contribution of analytical chemistry to security activities and to criminal investigation we find a common central idea: analytical chemistry supplies chemical information with the aim of helping decisions to be taken respecting a juridical framework. In the area of crime prevention, the probabilistic sensitivity and specificity of the techniques used can be limited because of the need to take decisions in a short time, as it happens during the control of people and luggage in airports, or in the activity to spot a criminal bomb factory. The acceptable degree of uncertainty is higher, when dealing with security problems, compared to criminal investigation, due to the limited time. When reporting chemical information as evidence in the Court uncertainty must be minimised, since the Court needs to establish the truth beyond any reasonable doubt.

Francesco Saverio Romolo
SAPIENZA University of Rome, Department of Anatomical, Histological, Forensic Medicine and Orthopedics Sciences - Legal Medicine Section

Gianni Giulio Vadalà
SICSS - Società Indagini, Consulenze Scientifiche e Sicurezza, Roma

references & notes

[1] R. Meyer, J. Köhler, A. Homburg, 2007, Explosives, Sixth Edition, Wiley-VCH & Co. KGaA, Weinheim.

[2] T. Urbansky, 1964, in Chemistry and technology of explosives, Vol. I-III, Pergamon Press, Member of Maxwell Macmillan Pergamon Publishing Corporation, Oxford, New York, Beijing, Frankfurt, Sao Paulo, Sydney, Tokyo, Toronto.

[3] R. Schulte-Ladbeck, P. Kolla, U. Karst, 2006, "Recent methods for the determination of peroxide-based explosives", in Anal. Bioanal. Chem., 386, 559-565.

[4] R.M. Burks, D.S. Hage, 2009, "Current trends in the detection of peroxide-based explosives", in Anal. Bioanal. Chem., 395, 301–313.

[5] M.S. Meaney, V.L. McGuffin, 2008, "Luminescence-based methods for sensing and detection of explosives", in Anal. Bioanal. Chem., 391, 2557-2576.

[6] International Civil Aviation Organization (ICAO), Working Paper: High-Level Conference on Aviation Security (HLCAS), Montréal, 12 to 14 September 2012 (last access 18th June 2014). http://www.icao.int/Meetings/avsecconf/Documents/WP 14/LIQUIDS, AEROSOLS AND GELS.en.pdf

[7] J. Yinon, 1999, Forensic and environmental detection of explosives, John Wiley & Sons, Chichester.

[8] A. Naquet, 1884, Legal Chemistry. A guide to the detection of poisons, examination of tea, stains, etc., as applied to chemical jurisprudence, Second edition, revised with additions. D. Van Nostrand Company, New York.

[9] A. Maehly, L. Strömberg, 1981, Chemical Criminalistics, Springer-Verlag.

[10] General Assembly of the United Nations, 1948, Universal Declaration of Human Rights, Article 3, http://www.un.org/en/documents/udhr/index.shtml#a3 (last access 28th June 2014).

[11] P. Kolla, 1996, "The application of analytical methods to the detection of hidden explosives and explosives devices", in Angew. Chem. Int. Ed. Engl., 36, 800-811.

[12] D.H. Fine, G.J. Wendel, 1994, "Sampling of explosives by means of the EGIS vapor/particle detector", in Proceedings of SPIE-The International Society for Optical Engineering, 2092, Substance Detection Systems, 131-136.

[13] H. Östmark, S. Wallin, H.G. Ang, 2012, "Vapor Pressure of Explosives: A Critical Review", in Propellants Explos. Pyrotech., 37, 12 – 23.

[14] M. Marshall, J. Oxley, 2009, "Detection of explosives by dogs," in Aspects of Explosives Detection, 1st ed., M. Marshall and J. Oxley, Eds., 27–38, Elsevier, Amsterdam, Netherlands.

[15] E. Linos, E. Linos, G. Colditz, 2007, "Screening programme evaluation applied to airport security", in BMJ, 335, 1290-1292.

[16] EU Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR), 2012, Health effects of security scanners for passenger screening (based on X-ray technology).

[17] ICPO Interpol, 2007, Bioterrorism Incident Pre-Planning & Response Guide.

[18] M.E. Germain, M.J. Knapp, 2009, "Optical explosives detection: from color changes to fluorescence turn-on", in Chemical Society Reviews, 38, 2543–2555.

[19] Y. Salinas, R. Martínez-Máñez, M.D. Marcos, F. Sancenón, A.M. Costero, M. Parra, S. Gil, 2012, "Optical chemosensors and reagents to detect explosives", in Chemical Society Reviews, 41, 1261–1296.

[20] Yáñez-Sedeño, et al., 2014, "Biosensors in forensic analysis. A review", in Anal. Chim. Acta, http://dx.doi.org/ 10.1016/j.aca.2014.03.011

[21] S. Girotti, S, Eremin, A. Montoya, M.J. Moreno, P. Caputo, M. D'Elia, L. Ripani, F.S. Romolo, E. Maiolini, 2010, "Development of a chemiluminescent ELISA and a colloidal gold-based LFIA for TNT detection", in Anal. Bioanal. Chem., 396, 687-695.

[22] S. Almaviva, S. Botti, A. Palucci, A. Puiu, F. Schnürer, W. Schweikert, F.S. Romolo, 2014, "Application of micro-Raman spectroscopy for fight against terrorism and smuggling", in Optical Engineering 53(4), 044113.

[23] S. Wallin, A. Pettersson, H. Östmark, A. Hobro, 2009, "Laser-based standoff detection of explosives: a critical review", in Anal. Bioanal. Chem., 395, 259–274 DOI: 10.1007/s00216-009-2844-3

[24] A. Pettersson, I. Johansson, S. Wallin, M. Nordberg, H. Östmark, 2009, "Near Real-Time Standoff Detection of Explosives in a Realistic Outdoor Environment at 55 m Distance", in Propellants Explos. Pyrotech., 34, 297 – 306 297 Full Paper.

[25] http://www.foi.se/en/Top-menu/Pressroom/News/2012/FOI-showcases-five-EU-projects-at-trade-fair-in-Germany/ (last access 28th June 2014).

[26] R.A. Potyrailo, N. Nagraj, C. Surman, H.Boudries, H. Lai, J.M. Slocik, N. Kelley-Loughnane, R.R. Naik, 2012, "Wireless sensors and sensor networks for homeland security applications", in Trends Analytical Chemistry, 40, 133-145.

[27] BONAS web site http://bonas.tekever.com (last access 28th June 2014).

[28] M.C. Kemp, 2013, "A review of sensor data fusion for explosives and weapons detection", in Proc. SPIE 8710, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XIV, 87100X (May 29, 2013); DOI: 10.1117/12.2015530

[29] J.S. Caygill, F. Davis, S.P.J. Higson, 2012, "Current trends in explosives detection techniques", in Talanta, 88, 14–29.

[30] A.D. Beveridge, 1992, "Development in the detection and identification of explosives residues", in Forensic Science Review, 4 (1), pp. 17-49

[31] J. Almog, 2006, "Forensic Science Does Not Start in the Lab: The Concept of Diagnostic Field Tests", in J. Forensic Sci., 51(6), 1228-1234.

[32] D. Royds, S. Lewis, A.M. Taylor, 2005, "A case study in forensic chemistry: The Bali bombings", in Talanta, 67, 262–268.

[33] D. Perret, S. Marchese, A. Gentili, R. Curini, A. Terracciano, E. Bafile, F.S. Romolo, 2008, "LC–MS–MS Determination of Stabilizers and Explosives Residues in Hand-Swabs", in Chromatographia, 68 (7-8), 517-524.

[34] S.A. Phillips, R. Hiley, 1999, "Proceedings of the workshop on explosives trace analysis methods", DERA, UK, April 1999, In Science & Justice, 39(4), 261-268.

[35] European Communities. Commission Decision of 12th August 2002 implementing Council Directive 96/23/EC concerning the performance of analytical methods and the interpretation of results. Official Journal of the European Communities 2002; L 221: 8-36.

[36] F.S. Romolo, L. Cassioli, S. Grossi, G. Cinelli, M.V. Russo, 2013, "Surface-sampling and analysis of TATP by gas chromatography/mass spectrometry", in Forensic Sci. Int., 224, 96–100.

[37] M.E. Sigman, C.D. Clark, T. Caiano, R. Mullen, 2008, "Analysis of triacetone triperoxide (TATP) and TATP synthetic intermediates by electrospray ionization mass spectrometry", inRapid Commun. Mass Sp., 22, 84-90.

Rilevamento di tracce di esplosivo mediante spettroscopia di plasma indotto da laser

Sono stati eseguiti studi comparativi delle righe spettrali del plasma prodotto su residui di esplosivi o interferenti organici. La distribuzione e lo spessore dei residui non erano uniformi, proprio come ci si deve aspettare nelle condizioni operative di interesse per la *security*, nelle quali lo strumento sarà testato durante le prossime campagne di misura. Questi studi hanno permesso di identificare i parametri spettrali che portano a una corretta classificazione dei residui per i dati acquisiti. In tutti i casi, la soglia di rilevamento stimata per gli esplosivi è compresa tra 0,1 e 1 ng.

Explosive's trace detection by laser-induced breakdown spectroscopy

Comparative studies of the line intensities from the plasma produced on residues from explosives or organic interferents were performed. The residues had not uniform distribution and thickness, as expected in real conditions for security applications, to be tested in forthcoming campaigns. These studies allowed identifying the spectral parameters for the correct residue classification within the acquired data set. In all the cases, the estimated detection threshold was between 0.1 ng and 1 ng of explosives.

DOI: 10.12910/EAI2014-87

■ *V. Lazic, A. Palucci*

Introduction

Field explosive detection is extremely important for homeland security. Although many explosive's detection techniques are well established, there is still the need and technological challenge for development of fast, in-situ screening sensors. One of the possibilities to recognize hidden explosives is through the detection of their dispersed particles. The handling and transportation of explosives has been shown to generate explosive traces on surfaces, which may subsequently be detected [1]. One of the most promising techniques for ultra-rapid, in-situ identification of materials is the laser-induced breakdown spectroscopy (LIBS) [2, 3], as it does not require any sample preparation. LIBS analyses demand no contact, making stand-off detection possible from up to 130 m [3].

LIBS is based on plasma generation by an intense laser pulse, which leads to atomization and ionization of the sample material. Spectral emission from the excited species in plasma is used for the identification and eventual quantification of the sample composition. Explosives are organic compounds, containing carbon, hydrogen, and oxygen, while nitrogen is present in almost all high explosives. Commonly, explosives are rich in N and O, and poor in H and C, with respect to

■ **Contact person: Violeta Lazic**
violeta.lazic@enea.it

other organic substances. LIBS spectra from energetic materials normally contain atomic lines from these four elements and molecular bands of CN and C_2 [3-6]. Molecular emission can be attributed both to the native C=C and C-N bonds [7, 8] and to recombination in plasma [9]. Rapid LIBS detection of energetic materials is normally performed in air surroundings, so the interference from air components on the spectra must be taken into account. Classification of organic compounds by LIBS can be performed by comparison between the sample spectra and the previously established library, or by comparing line intensity ratios from H, C, N and O [3-6]. In this latter case, a procedure for explosive recognition is based on properly constructed algorithms, or on chemometric methods.

Similarly to LIBS, Raman spectroscopy might be applied for stand-off explosive detection. The Raman technique is highly discriminant, being based on molecular detection where each substance has its characteristic spectra. However, the Raman technique deals with low-signal intensities and the estimated explosive detection limit is in the order of 1-100 µg, which is not always sufficient for trace detection. Differently, LIBS is highly sensitive with respect to Raman, but it is less selective and requires further fundamental studies in order to understand and establish the most discriminant spectral features of explosives compared to the common organic materials.

The final scope of this work is to establish the most appropriate procedure for explosive trace recognition by LIBS, later to be exploited for in-field operation, as required by the FP7 project EDEN (End-user driven DEmo for cbrNe). The instrument for remote explosive detection is under construction and is illustrated in Figure 1. The LIBS sensor was designed to perform measurements at distances between 7.5 m and 30 m through the scanning of surface areas chosen by the operator, with the help of integrated viewing systems.

In the present work we present the results from LIBS measurements on residues of nine types of explosives and of some common organic materials. The random presence of residues on the target corresponds to conditions expected in real situations.

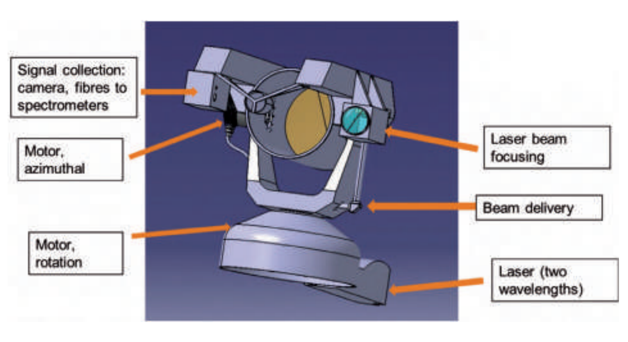


FIGURE 1 Laser system for remote explosive detection

Experimental

Measurements were performed by the LIBS prototype system developed by the industrial company IPAC (Austria) in the frame of the ISOTREX project (FP6). The system employs Nd:YAG laser from Quantel (Model Ultra 50) operated at 1064 nm. The laser pulse width was 8 ns and the laser energy was fixed at 50 mJ. The laser beam of a 3 mm diameter was focused onto the sample surface by two quartz lenses with effective focal length of about 90 mm, thus producing the laser spot of diameter 0.22 mm (Fig. 1). The corresponding energy density averaged across the laser spot was of about 130 J/cm^2, which is 3.6 times higher than in our previous experiment [6], with the advantage of achieving a higher degree of atomization of the organic compound in the plasma.

The plasma emission was collected by two optical systems containing focusing optics and fiber bundles [10]. At one end, the bundle was separated into single fibers, and each of them was connected to one of the six spectrometer channels (StellarNet). A single channel, with 0.1 nm spectral resolution, covers a bandwidth of about 100 nm, and it is equipped with a 2048 Photo-Diode Array (PDA). Each spectrometer channel was triggered externally and simultaneously with the laser flash lamp. The minimum integration time used here was 30 ms. The spectrometers cover the 200-800 nm spectral range. After one laser shot, the whole spectrum was saved for further analysis by custom written programs under Labview.

A sample was placed on an X–Y micrometric table, and

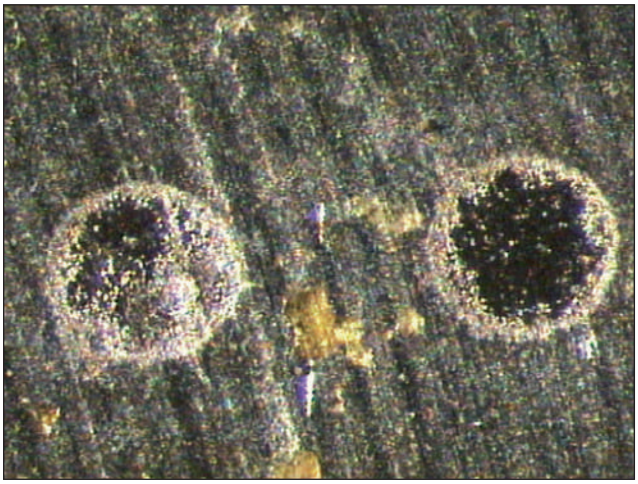


FIGURE 2 Photo of laser-induced craters (0.22 mm diameter) in the presence of TETRYL residues, here yellow

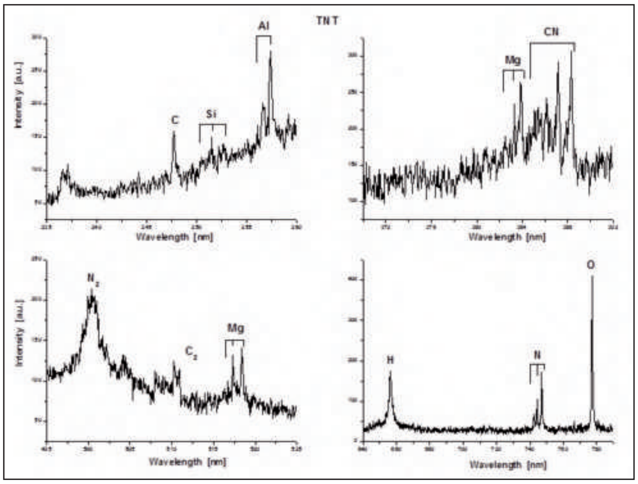


FIGURE 3 Characteristic spectral parts of TNT traces on aluminium support; Si, Mg and Al lines belong to the support

shifted by 0.5 mm after each laser pulse. The support material for residues was aluminum (Anticorodal), roughly machined (Fig. 2) and cleaned in an ultrasound bath, first with pure acetone and then with distilled water. All the explosives considered, except DNT, are standard solutions with concentration of 1.0 mg/ml or 0.1 mg/ml (TATP) in methyl- or ethyl alcohol, or acetonitrile. DNT was purchased in the form of crystal grains and dissolved in pure acetone before placing it onto support. Small droplets of solution containing explosives spread themselves over the aluminum surface and were left to evaporate thermally, leaving unevenly distributed residues (Fig. 2). Other analyzed, not energetic materials (diesel, pure paraffin wax, and hand cream) were directly distributed over the support in thin layers of uncontrolled thickness. After the initial measurements on the interferents, the substrate was wiped out with a tissue in order to reduce the residue thickness. This operation was repeated a few times.

Results and discussion

The spectra obtained on organic residues always contained the emission lines of aluminium, thus indicating the support ablation, too. A typical LIBS spectrum on organic residues is shown in Figure 3. The plasma intensity also from the clean support exhibits fluctuations [6, 10] due to the surface roughness with structures comparable to the spot size and due to laser energy instabilities. In case of the residues, a more intense LIBS signal corresponds to a smaller sample amount inside the laser focal spot.

In our previous work [6] the initial data set was elaborated in three different ways attempting to explosives from interferents:

1) Principal component analysis (PCA) which includes line ratios O/N, O/C, H/C, N/C, N/H and O/H
2) Plot of the line intensities H/N as a function of Al
3) PCA analysis with the line ratios (1) plus parameter A, which considers a possible recombination between C and N in the plasma, and is defined as:

$A= I(C_2)-2*K_1I(N)– I(CN) + K_2I(C)$

Where coefficients K_1 and K_2 were weighted as 0.6 and 2.0, respectively, to produce similar contribution of the terms.

The results of the classification by the three methods are shown in Table 1, where the highest score is marked with red. From here, it could be noted that beside the interferents, five out of nine explosive could be 100% correctly classified by LIBS. Differently, EGDN and DNT produced a false negative of about 20%, while NG and TATP had a high error rate with all the three methods applied. The false negatives always occurred for relatively thick residues; the corresponding plasma temperature, measured through the Boltzmann's plot, was also for 3000 K with respect to the plasma on thin residue [10]. The plasma temperature affects not only the excitation of the emission lines but is also related to the molecule fragmentation and chemical reactions in the plasma.

All the previous works by other research groups considered that the plasma produced on explosives was stoichiometric, i.e., the intensities of the characteristic lines from C, H, N, O, CN and C_2 were proportional to the sample amount. The corresponding classification procedures were based on this assumption, which also means that the ratios of the characteristic spectral lines are stable in the plasma.

In the present experiment, where the laser irradiance was relatively high and favorable to achieve a more complete fragmentation of organic molecules, we observed the following:

Name	Method 1	Method 2	Method 3
EGDN	65	81	68
NG	0	3	39
RDX	95	100	59
TNT	100	100	100
DNT	79	36	64
PETN	100	100	100
HMX	95	100	95
TETRYL	100	96	100
TATP	4	4	54
Diesel oil	100	100	100
Paraffin wax	100	100	100
Grease lubricant	100	100	100
Glue LOCTITE	100	100	100
Hand cream	100	100	100
Support	100	100	100

TABLE 1 Percentage of correct sample classification by LIBS (explosive or non-explosive) according to the methods 1-3 (cf. text above)

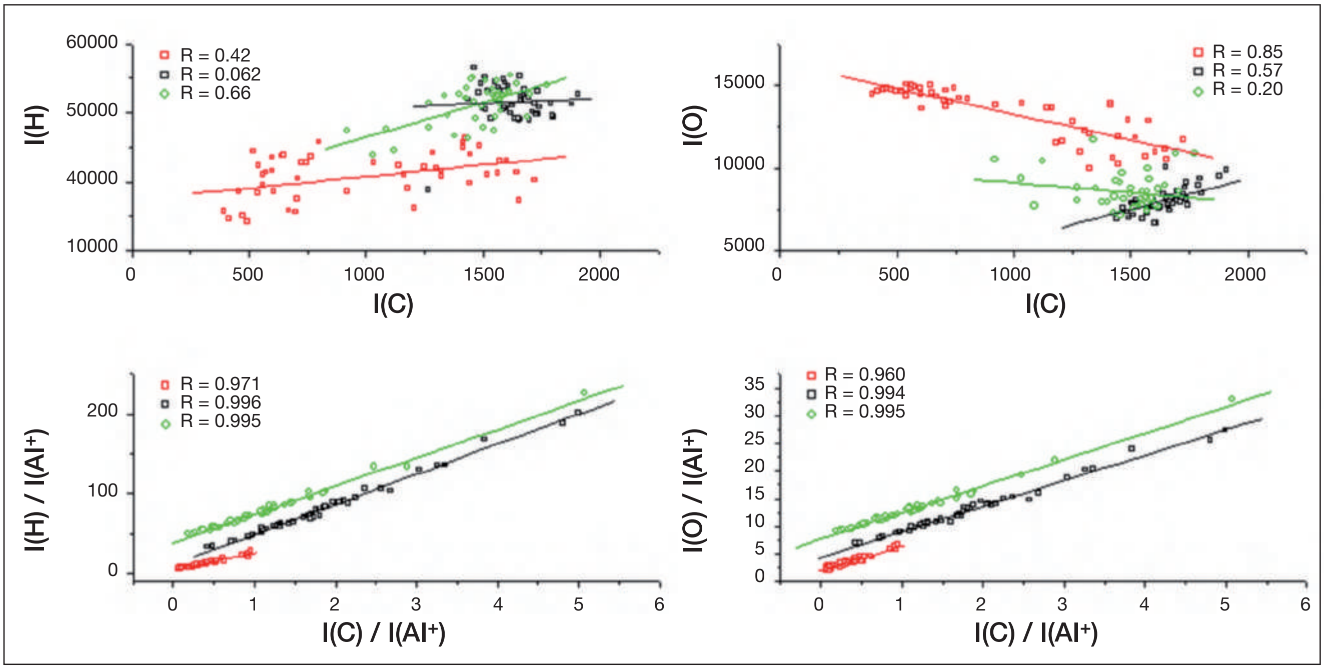


FIGURE 4 H and O emission intensities from TNT (red), diesel (black) and paraffin (green) residues as a function of atomic C emission: top — raw data; bottom – after normalization; the points of diesel and paraffin are shifted vertically [10]

Explosive	H(O)	N(O)	N(H)	O(C)	N(C)	H(C)	Total	% of correct classif.
TATP	- / -	- / -	- / -	+ / -	- / -	- / -	1 / 0	4
NG	- / -	- / -	- / -	- / -	+ / -	- / -	1 / 0	0
EGDN	- / -	- / -	- / -	+ / -	+ / +	+ / -	3 / 1	65
RDX	+ / +	- / -	- / -	- / -	+ / -	+ / -	3 / 1	95
DNT	+ / +	- / -	- / -	- / -	+ / -	+ / +	3 / 2	79
HMX	+ / +	- / -	+ / -	+ / -	+ / -	+ / +	5 / 1	95
TETRYL	- / +	- / -	- / -	+ / -	+ / +	+ / +	3 / 3	100
PETN	+ / +	- / -	- / -	+ / -	+ / +	+ / +	4 / 3	100
TNT	+ / +	- / -	+ / -	+ / -	+ / +	+ / +	5 / 3	100

TABLE 2 Capability to discriminate explosives (+ for yes, - for no) through the intercepts/slopes, respectively, of the linearly fitted functions involving different emission lines; the last column compares the percentage of correct classifications previously obtained by PCA (Table 1, method 1)

1) In the presence of carbon in the plasma, atomic emissions from O and N are clearly reduced; this indicates that O and N atoms are lost in some chemical reactions involving products of fragmented organic molecule.
2) There is a striking anti-correlation between line intensities from N, O, and Al^+ (from the support) with respect to the emission from atomic carbon. Simultaneously, H emission follows fluctuations of C line intensity, as expected from the residue molecular formula.
3) The line intensity ratios change even for one order of magnitude from one sampling point to another; consequently, averaging the spectra in the attempt to classify organic residues is not meaningful.
4) The LIBS plasma generated on organic samples is not stoichiometric; this was particularly evident from very different line intensity ratios (up to 60%) on RDX and HMX, which have the same stoichiometry in the molecular formula.
5) Ionic emission intensity, here of Al^+, is a good indicator of the plasma temperature and the electron density. The line intensity ratio of Al^+/Al changes with the residue thickness, and the measured electron density was always lower in the spectra with more intense Al^+ lines, corresponding to a smaller quantity of the residue, see point 2) [10].

Based on the facts above, it was possible to establish the normalization procedure which linearizes the data set (Fig. 4 bottom) starting from weakly correlated data (Fig. 4 top). The slopes and intercepts of different linearized functions, related to H, N, O and C emission lines, were calculated both for explosives and interferents, and those marking the difference among them are shown in Table 2. The intercept indicates the function value for very thin residues.

From Table 2, it can be observed that the functions H(O), H(C) and N(C) are the most important features for explosive classification. Although the LIBS-measured ratio O/N was also considered as an indicator of the presence of explosives [3, 11-12], the results shown in Table 2 demonstrate that the function O(N) does not contribute to the discrimination at all. Both atomic oxygen and nitrogen are depleted in the presence of carbon in the plasma, and anomalous O/N ratio in the molecules of the explosives is not reproduced in the LIBS spectra. From the intercepts of the function N(C), all residues containing nitrogen are clearly distinguished from interferents. This was true also for nitroglycerin, which is difficult to discriminate by LIBS. From the slopes of O(C) it was not possible to discriminate the residues; however, the intercepts are again indicative of most of the explosives, including TATP. Hydrogen emission was always more intense on thicker residues. It is well known in literature that detaching hydrogen needs less energy than fragmenting the whole organic molecule [13]. For most of the explosives examined here, the slope of H(C) is lower than for interferents, indicating that a detachment of hydrogen from the mother molecule in the weak plasma (thick residue) is less efficient.

The results summarized in Table 2 show that some intercepts of the considered atomic functions allow distinguishing all the examined explosives from the interferents; the corresponding slopes are less indicative. This also signifies that the organic residues can be more easily classified when present in very thin layers (close to the intercept points) or under high laser irradiance, where the plasma temperature is high and molecular fragmentation is efficient. The TNT residue is the easiest to discriminate by LIBS as it differs from the interferents in eight of the examined twelve functions. Differently, TATP and NG are very difficult to detect by LIBS since they have only one function intercept out of the ranges belonging to the interferents. These results are in good agreement with the percentages of correct classifications previously obtained on residues of the same explosives [6], where PCA analyses were performed considering the next line intensity ratios: O/N, O/C, H/C, N/C and O/H.

When probing the residues by laser, the non-uniform distribution of the sample must be taken into account, and this generates LIBS spectra with strongly variable line intensities and their respective ratios. However, thanks to a good correlation between the characteristic line intensities after proper normalization (Fig. 4, bottom row), a 100% correct classification of all the residues here considered was obtained by the simple procedure described in the following:

1) acquisition of a sufficient number of single-shot spectra (for example, more than 30 spectra);
2) normalization of C, H, N and O line intensities on ionic emission (here on Al^+) in all the individual spectra;
3) linear fitting of the normalized functions H(O), N(H), O(C), N(C) and H(C), and retrieving of their slopes and intercepts;
4) verifying if one or more of the calculated slopes and intercepts fall inside the limits for explosives.

For the organic residues distributed over support materials other than here, the data linearization could be performed by involving different parameters related to the plasma condition, as for example other ionic lines (like C^+) or continuum spectral distribution. Each type of normalization requires evaluating the errors in the fitting, before placing the limits that separate explosives from interferents.

Conclusions

In the presence of non-uniform organic residues, as expected in real-field conditions, the LIBS plasma parameters vary from one sampling point to another. This also leads to changes in the laser-induced fragmentation pathways and in chemical reactions inside the plasma. The characteristic line intensities and their ratios change up to one order of magnitude from one spectrum to another. The plasma induced on organic materials is not stoichiometric.

The organic residues can be more easily classified by LIBS when present in very thin layers or exposed to high laser irradiance, where the plasma temperature is high and molecular fragmentation is efficient. Among the examined explosives, the easiest to identify in air by LIBS is TNT, followed by HMX, PETN and TETRYL. The most difficult to discern are NG and TATP, having only one function each that distinguish them from other organic residues.

These results of the present studies will be exploited for building up the classification procedure for the stand-off LIBS instrument under development. The chosen approach will be tested and validated over a larger number of residues, and placed on different substrates than here.

Violeta Lazic, Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation -
Diagnostics and Laser Metrology Laboratory

references & notes

[1] D.J. Phares, J.K. Holt, G.T. Smedley, R.C. Flagan, 2000, “Method for characterization of adhesion properties of trace explosives in fingerprints and fingerprint simulations”, in J. Forensic Sci., 45, 774–784.

[2] J.D. Winefordner, I.B. Gornushkin, T. Correll, E. Gibb, B.W. Smith, N. Omenetto, 2004, “Comparing several atomic spectrometric methods to the super stars: special emphasis on laser induced breakdown spectrometry, LIBS, a future super star”, in J. Anal. At. Spectrom.,19, 1061–1083.

[3] C. López-Moreno, S. Palanco, F. DeLucia Jr., A.W. Miziolek, J. Rose, R.A. Walters, A. Whitehouse, J.J. Laserna, 2006, “Test of a stand-off laser-induced breakdown spectroscopy sensor for the detection of explosive residues on solid surfaces”, in J. Anal. At. Spectrom., 21, 55–60.

[4] J.L. Gottfried, F.C. De Lucia Jr, C.A. Munson, A.W. Miziolek, 2008, “Strategies for residue explosives detection using laser-induced breakdown spectroscopy”, J. Anal. At. Spectrom., 23, 205-216.

[5] J.L. Gottfried, F.C. De Lucia Jr., C.A. Munson, A.W. Miziolek, 2007, “Double-pulse standoff laser-induced breakdown spectroscopy for versatile hazardous materials detection”, in Spectrochim. Acta Part B, 62, 1405–1411.

[6] V. Lazic, A. Palucci, S. Jovicevic, C. Poggi, E. Buono, 2009, “Analysis of explosive and other organic residues by laser induced breakdown spectroscopy”, in Spectrochim. Acta Part B, 64, 1028–1039.

[7] A. Portnov, S. Rosenwaks, I. Bar, 2003, “Emission following laser-induced breakdown spectroscopy of organic compounds in ambient air”, in Appl. Optics , 42, 2835-2842

[8] M. Baudelet, M. Boueri, J. Yu, S.S. Mao, V. Piscitelli, X. Mao, R.E. Russo, 2007,“Time-resolved ultraviolet laser-induced breakdown spectroscopy for organic material analysis”, in Spectrochim. Acta Part B, 62, 1329–1334.

[9] V.I. Babushok, F.C. DeLucia Jr., P.J. Dagdigian, J.L. Gottfried, C.A. Munson, M.J. Nusca, A.W. Miziolek, 2007, “Kinetic modeling study of the laser-induced plasma plume of cyclotrimethylenetrinitramine (RDX)”, in Spectrochim. Acta Part B, 62, 1321–1328.

[10] V. Lazic, A. Palucci, S. Jovicevic, M. Carpanese, 2011, “Detection of explosives in traces by laser induced breakdown spectroscopy: Differences from organic interferents and conditions for a correct classification”, Spectrochim. Acta Part B, 66, 644–655.

[11] J.L. Gottfried, F.C. De Lucia Jr., C.A. Munson, A.W. Miziolek, 2007, “Double-pulse standoff laser-induced breakdown spectroscopy for versatile hazardous materials detection”, in Spectrochim. Acta Part B, 62, 1405–1411.

[12] F.C. De Lucia Jr., R.S. Harmon, K.L. McNesby, R.J. Winkel Jr., A.W. Miziolek, 2003, “Laser induced breakdown spectroscopy analysis of energetic materials”, in Appl. Opt., 42, 6148–6152.

[13] P.K. Dutta, Y. Talmi, 1981, “Desorption and fragmentation studies of organic molecules by laser-induced mass spectrometry”, in An. Chim. Acta, 132, 111–118.

Rilevamento di tracce di materiali energetici tramite spettroscopia Raman a fini antiterroristici

Il rilevamento di esplosivi a livello di traccia ha acquisito maggiore importanza negli ultimi decenni, in particolare da quando i terroristi hanno sempre più preso di mira obiettivi civili e alcuni tipi di esplosivi possono essere preparati con ingredienti facilmente reperibili.
Tra le tecnologie di rilevamento attualmente disponibili, la spettroscopia Raman è un potente strumento di analisi per lo studio di materiale forense, in grado di visualizzare e analizzare piccolissime quantità di campioni, dell'ordine di picomoli, con la relativa specificità chimica. Grazie alla capacità di individuare composti organici e inorganici, volatili o non volatili, e spesso di esaminarli in loco, l'interesse circa l'utilità della tecnologia Raman è divenuto ancora maggiore. Nel presente articolo sono illustrate due applicazioni della tecnologia Raman, sviluppate dall'ENEA, per il rilevamento di tracce di esplosivi: il rilevamento prossimale Raman LIDAR (Laser Imaging Detection and Ranging), che permette di individuare tracce di esplosivo con un unico fascio laser UV in condizioni di sicurezza per gli occhi, e la tecnica spettroscopica SERS (Surface Enhanced Raman Spectroscopy), che consente di rilevare tracce di molecole e sostanze in quantità fino a picogrammi.

Raman spectroscopy for detecting trace amounts of energetic materials for counterterrorism issues

The detection of trace levels of explosives has become more important in the last decades as terrorists have increasingly targeted civilians and some type of explosives can be prepared from easily obtainable ingredients.
Among the detection technologies available, Raman spectroscopy is a powerful analytical tool for the study of forensic materials since it can view and analyze small samples down to picomole quantities with chemical specificity. The ability to analyze both organic and inorganic compounds, either volatile or nonvolatile species, and to often examine them in situ has also increased the interest in the utility of Raman. In this work two applications of Raman-based techniques, developed at ENEA, are presented for the detection of trace amounts of explosives: Raman LIDAR (Laser Imaging Detection and Ranging) proximal detection, capable of trace detection of explosives with a single UV laser shot in eye-safety conditions, and Surface Enhanced Raman Spectroscopy (SERS), capable of detecting molecules and substances in trace quantities down to picograms.

DOI: 10.12910/EAI2014-88

■ *S. Almaviva, F. Angelini, R. Chirico, G. Dipoppa, I. Menicucci, M. Nuvoli, A. Puiu, A. Palucci, S. Botti, L. Cantarini, A. Rufoloni*

■ Contact person: Antonio Palucci
antonio.palucci@enea.it

Introduction

In the last decades there have been several terroristic attacks with improvised explosive devices (IED) that have raised the need for new instrumentation and homeland security applications, to obtain a reliable and effective means to fight against terrorism. Public transportation has been around for about 150 years, yet terroristic attacks against buses, trains, subways, etc. are a relatively recent phenomenon [1] that takes on different dimensions, depending on the countries' peculiarities in the global scenario (Fig. 1). Since 1970, transportation has been an increasingly attractive target for terrorists (Fig. 2).

An attack with an IED is performed with a "homemade" bomb and/or destructive device, which can come in many forms, ranging from a small pipe bomb to a sophisticated device. IEDs can be: carried or delivered in a vehicle; carried, placed, or thrown by a person; delivered in a package; or concealed on the roadside. Many commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide, can be used as explosives, and other materials, such as nails, glass, or metal fragments, can be used to increase the amount of shrapnel propelled by the explosion [3].

Many precursors to IED can be easily purchased without any authorization from chemical supply stores, retail stores selling beauty supply products, groceries, and swimming pool supplies. Most of the substances classified as chemical explosives generally contain oxygen, nitrogen and oxidizable elements, such as carbon and hydrogen. Chemical explosives are generally dense and have high oxygen and/or nitrogen content to react with sufficient rapidity and to maximize the working fluid (i.e., gas) generated in the explosion [3]. The most common functional group in military explosives is NO_2. That functionality can be attached to oxygen ($O\text{-}NO_2$) in the nitrate esters (PETN), to carbon ($C\text{-}NO_2$) in the nitroarenes (TNT) and nitroalkanes (Nitromethane), and to nitrogen ($N\text{-}NO_2$) as in the nitramines (RDX). Some organic peroxides, such as TATP and HMTD, are popular amongst terrorists as they are powerful initiators that can be easily prepared from ingredients readily available. Azides are also powerful primary explosives commonly used as initiators (commercial detonators) in civilian and military operations, therefore they could be potentially used by terrorists as initiators for IEDs. Elemental ratios for some common basic explosives are reported in Figure 3.

Among the detection technologies available, Raman-based spectroscopy [4] has gained consensus as a potential tool for detecting trace explosives because of its high discrimination capabilities and extremely appealing application in remote sensing [5] and in-situ thanks to the implementation of nanostructured roughened noble-metal substrates [6]. The Diagnostics

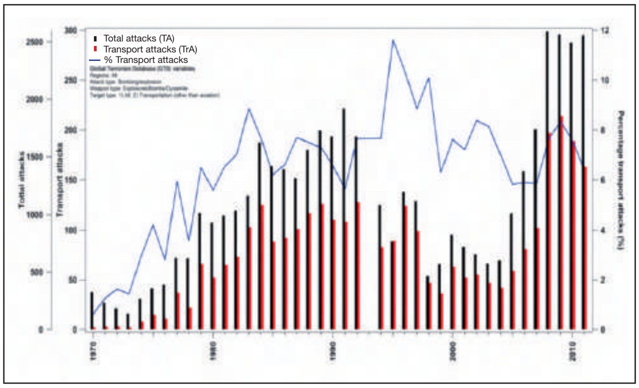


FIGURE 2 Total terroristic attacks and attacks against transportation using energetic material as weapon
Source: [2]

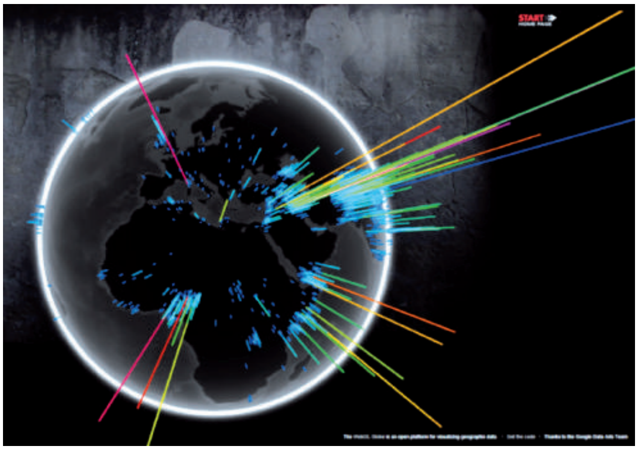


FIGURE 1 Pictorial view of the global scenario of terroristic attacks in Europe and Africa
Source: [2]

and Metrology (DIM) Laboratory have successfully investigated both techniques, developing a proximal LIDAR trace detection of explosives (10 cm – 200 m, NATO classification) and the Surface-Enhanced Raman-Scattering (SERS) [7, 8] technique for a handheld device. While the LIDAR system has the main aim of remotely monitoring trace compounds without any contact with the possible suspect person, the SERS device can be applied to the detection of very low content particles, dispersed in the environment in different contests as in the bomb factory discovery down to picograms quantities.

Raman LIDAR proximal sensor

The RADEX (RAman Detection of Explosives) system is a Raman-based technology to detect trace explosives considering the constraint of the maximum permissible laser exposure of the human cornea (3 mJ/cm^2 for a 266-nm laser).

The expected scenario was the monitoring of dispersed explosive compounds on people, either on their accessible clothes or on their personal objects, passing through a high-transit corridor such as, e.g., that in a metro station.

The operational principle of the RADEX system is the following (Fig. 4): an eye-safe laser beam is focused on the target and the Raman scattered radiation, emitted from the illuminated surface, is collected by a telescope and imaged onto the entrance of a Raman spectrometer. The radiation is then analyzed, giving a spectrum suitable for the explosive detection and identification.

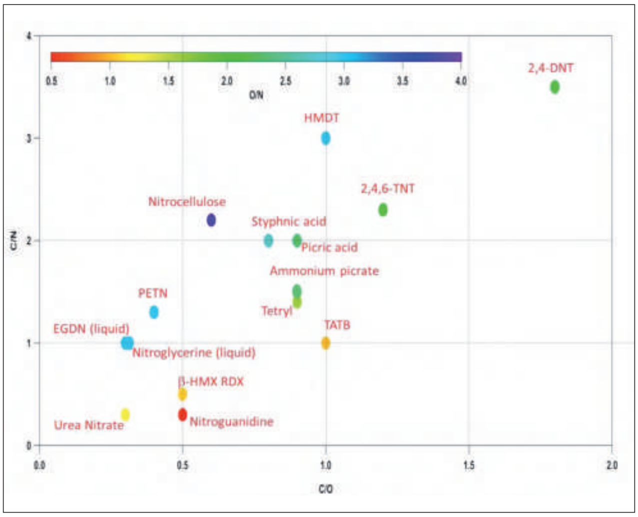


FIGURE 3 Elemental ratios of energetic materials

The apparatus was developed in the context of the STANDEX (STANdoff Detection of EXplosives) program (NATO Science for Peace and Security Program) [9] and it was part of an explosive warning system that includes the fusion of complementary detection sensors, designed to work in a mass transit infrastructure such as a metro station. The main features of the system are the use of technologies without having a physical contact with passengers, and a real time response.

The STANDEX program also included the demonstration of the system ability to automatically and discreetly detect and localize a hidden and mobile explosive in

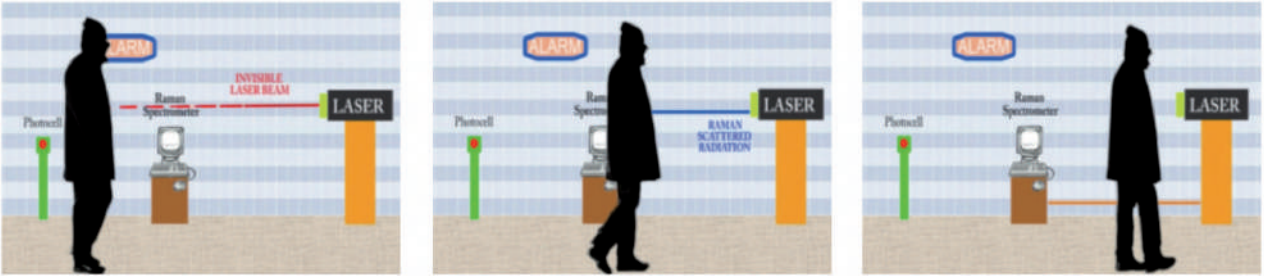


FIGURE 4 The operational principle of RADEX

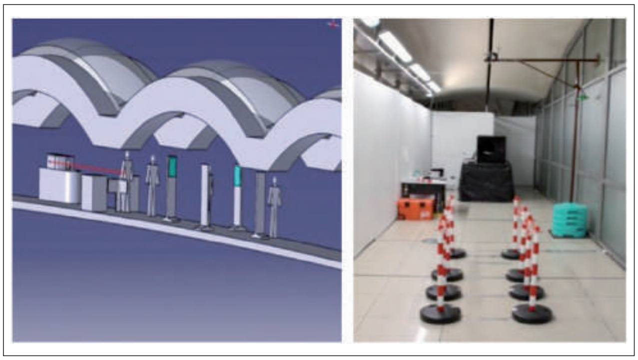


FIGURE 5 3D model of the Layout of the RADEX system on the footbridge and the RADEX set-up during the trials

real conditions of use, during a realistic phase of tests, in the metro station *Bibliothèque François Mitterrand* (the Big City Trials project).

The trials were performed by using real traces of explosive materials and with environmental conditions similar to those of a metro station, to ensure that the technology was compatible with the hard environmental conditions met inside large public transport stations, to validate the detection performances in an operational environment, and to assess the potential capabilities of the prototype to work together with the other instrumentation in a complex alarm system.

The RADEX prototype was placed on the footbridge of the BFM metro station as shown in Figure 5, looking into the direction opposite to the passenger flow with the laser placed at the specified height of 1.15 m from the ground. The corridor was delimited in order to guide the passengers in the direction of the instrument. At the end of the delimitated corridor, optical sensors were used to simulate a gate in order to synchronize the laser emission with the transit of a passenger.

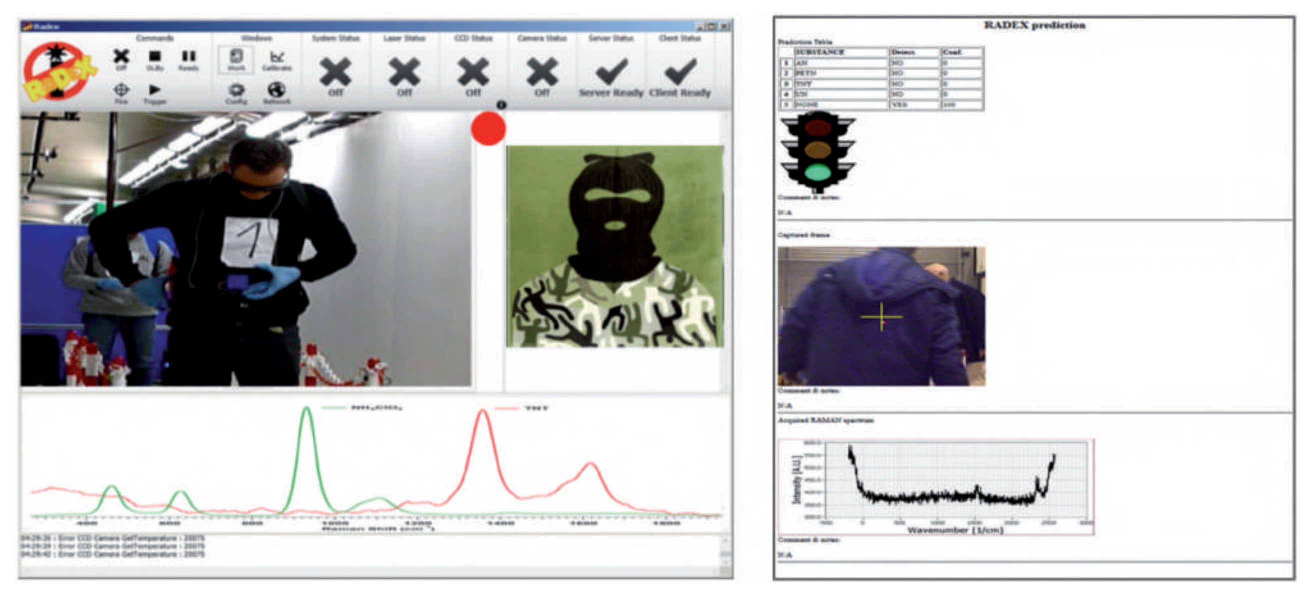
An on-line data analysis algorithm was implemented for the acquisition software in order to identify the substances in real time.

The safety requirements of the system demand that the identification of substances be performed on a single shot of low energy (energy density less than 3 mJ per square centimeter) in the UV region. For this reason, along with the fact that the echo is revealed at about 6 m from the target, the signal is very low although the system was optimized in order to lose as less energy as possible between the mirror and the CCD. Integration over more laser shots is not possible, and the analysis must be performed with sufficient reliability on each shot. The CCD was cooled to -70 °C in order to minimize the thermal noise and maximize the signal-to-noise ratio. Nevertheless, classical approaches for substance identification - based on multivariate analysis of spectral region - did not work with these noisy data, hence an original and alternative approach to data analysis was chosen. The raw signal is preprocessed to clean the spectra from noise, background and, eventually, fluorescence. The Ricker wavelet (also known as 'Mexican hat') was used as convolution kernel to calculate a special transform of the spectrum. The properties of this wavelet make the transform able to cut off both high frequency noise and low frequency trend, leading to a much easier analysis of the spectrum.

In order to avoid the classical scheme of peak recognition, based on the minimization of a some kind of distance in a suitable space between the spectrum under recognition and a reference database, a fuzzy approach is adopted. At the end of the fuzzy process, the percentage of presence of referenced species is provided, whereas the layout of the acquisition software provides the following information to the operator along with other valuable information acquired (Fig. 6): real time image from the videocamera of the instrument, the camera snapshot of the analyzed person, the acquired Raman spectrum, the logging data and the traffic light showing the analysis results.

The developed software is user-friendly for the operator, since only few preliminary steps are needed for the daily calibration, and the response given is "threat" or "no threat", indicated with a red or green signal, respectively.

The implemented software allows to use the apparatus either as stand-alone or in a more complex warming system, where the information provided by several instruments is collected and processed by a Data Merging and Alert System (DAMAS). Each time the DAMAS sent a "shot" command after the identification of a suspect person, the RADEX system automatically



RADEX prediction

Prediction Table

	SUBSTANCE	Detect.	Conf.
1	AN	NO	0
2	PETN	NO	0
3	TNT	NO	0
4	UN	NO	0
5	NONE	YES	100

Comment & notes:

N/A

Captured frame

Comment & notes:

N/A

Acquired RAMAN spectrum

Comment & notes:

N/A

FIGURE 6 Layout of the acquisition software and the first version of the web server with details of an incident report

sent an eye-safe laser shot when the potential bomber passed through the gate. The Raman signals produced by the target area were acquired and compared with those included in the database to figure out the presence of explosive traces. Then, the acquired information and the relevant response, were sent in real time to DAMAS (Fig. 7).

During the trials the following energetic materials were tested: ammonium nitrate, urea nitrate, TNT, PETN. Different fabrics (natural and synthetic) were used as a substrate for the deposition of energetic materials. Samples of traces of explosives on fabrics were prepared by the Fraunhofer Institute for Chemical Technology ICT using a piezoelectric Nano-PlotterTM (PNP, GeSIM, Germany). The PNP can deliver a precise number of droplets on a well-

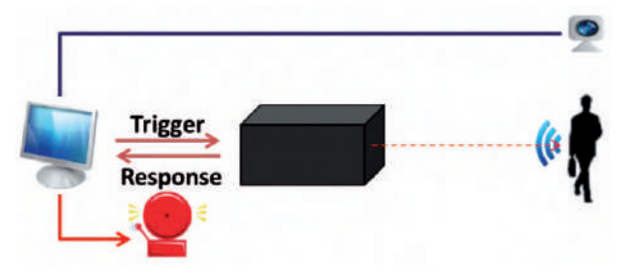


FIGURE 7 The schematic representation of the DAMAS-RADEX communication

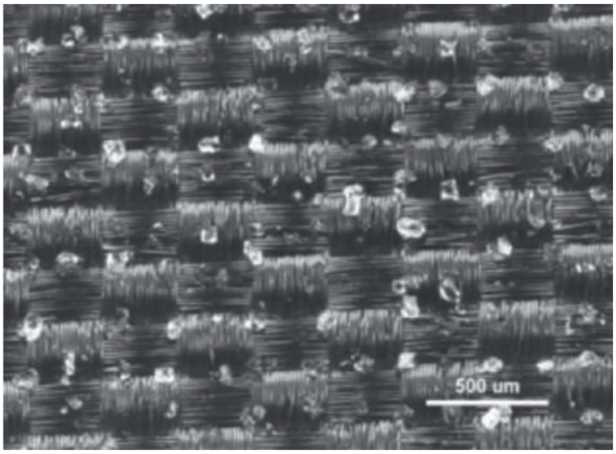


FIGURE 8 Energetic material deposited on the surface of synthetic fabrics with a piezoelectric Nano-Plotter^{TM}

defined surface (Fig. 8). This method provides a more uniform surface coverage with the analyte also for low surface densities (down to few µg/cm^2), as requested by the project.

Surface Enhanced Raman Spectroscopy (SERS)

At present the SERS enhancement mechanism appears to derive from two separate contributions: 1) an electromagnetic enhancement and 2) a chemical enhancement. The former comes through the electromagnetic interaction of light with metals, which produces large amplifications of the laser field through excitations generally known as plasmon resonances [10, 11, 12]; the latter corresponds to any modification of the Raman polarizability tensor upon adsorption of the molecule onto the metal surface [8 - 11].

The SERS technique has been implemented in the framework of the EC FP7 BONAS project [13], coordinated by DIM, in order to support the project partner Sersetech to develop a portable device.

Methodology

SERS substrates composed of arrays of inverted pyramidal pits (Klarite, Renishaw UK) have been implemented. A silicon nanostructure, produced by electron beam lithography, has been successively covered by a layer of gold deposited with the spattering technique [14]. In Figure 9, a sketch and a Scanning Electron Microscope (SEM) image of the substrate are shown.

Raman spectra were acquired with a table-top Raman system suitable for Raman and NIR measurements. For Raman measurements, it attaches via an optical fiber to an optical microscope, which in turn is attached to a diode laser source emitting at 785 nm. The detector is an un-cooled CCD. NIR excitation strongly reduces the sample fluorescence and the gold plasmonic frequency resonance is located near this spectral region [15]. The laser power was set at 180 mW on the samples while the acquisition time was 10 s. The scanned area, and therefore the sampled quantity depend on the objective used. In the case of the present measures, the laser beam was focused through the 20x objective, that means a laser spot of 90 µm diameter and an energy density of about $11.7 \cdot 10^3$ J/cm^2.

Results

Raman spectroscopy provides a unique spectral 'fingerprint' of any molecule, hence each spectrum is molecularly specific and contains key signature bands that can be used for unambiguous identification [16]. The SERS spectra of the explosives PETN, RDX, TNT, EGDN in the spectral region 250–2500 cm^{-1} are shown in Figure 10. Also, Table 1 lists the Raman wavenumbers and vibrational assignments of the principal characteristic bands of these explosives, which can be used to uniquely identify each substance [16, 17, 18, 19, 20, 21]. The comparison of the acquired spectra with the reference spectra showed that the

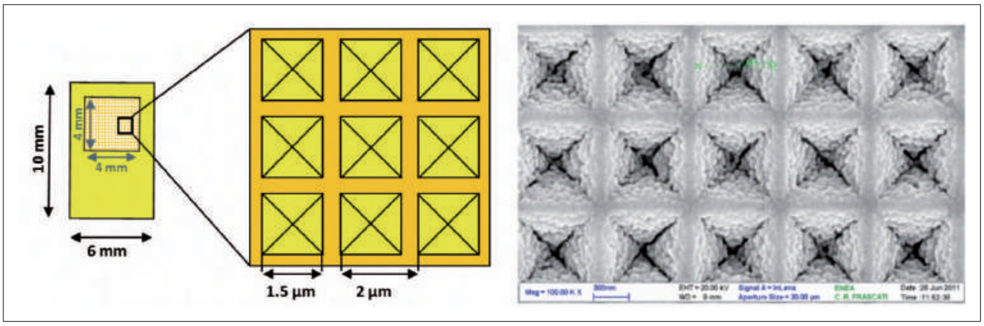


FIGURE 9 (left) Sketch of the SERS substrates. (right) SEM images of a portion of the SERS substrate. It is possible to recognize the inverted pyramidal pits

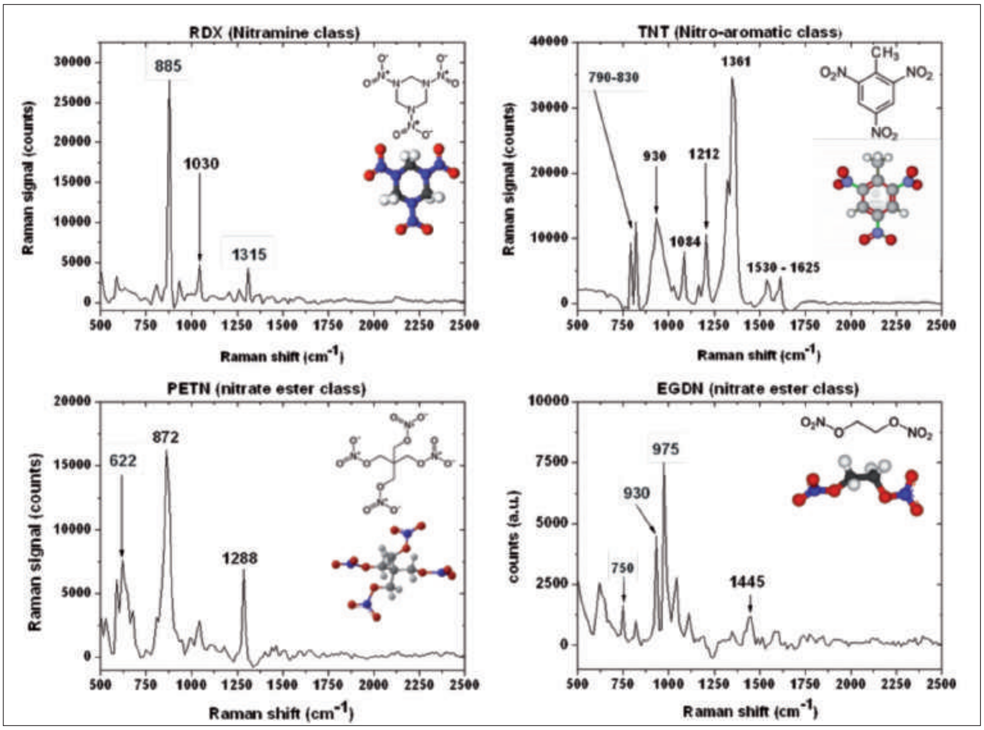


FIGURE 10 SERS spectra of PETN, RDX, TNT, EGDN. The mass probed by laser is about 200 pg for each substance. The acquisition time is 10 s. The laser power is set to 180 mW

Explosive	Wavenumber (cm^{-1}) vibrational assignments	Reference
PETN	1290, [ν_s (NO_2)] 871, [ν_s (O–N)]	[17]
EGDN	1600, [ν_{as} (NO_2)] 979, [C-O stretching] 941, [C-H_2 vibration] 756, [O-NO_2 umbrella]	[18]
TNT	1540, [ν_{as} (NO_2)] 1360, [ν_s (NO_2)] 1212, [C-H breathing] 790-822, [(NO_2) scissor] 796-827, [C-H bending]	[16]
RDX	1584, [ν_{as} (NO_2)] 1361, [ν_s (NO_2)] 1318, [C-H_2 wagging] 1260, [C-H_2 scissoring] 887, [C-N-C ring] 592, [O-C-O stretching]	[19, 20, 21]

TABLE 1 Wavenumbers and vibrational assignments of the principal characteristic bands observed in the explosive spectra

substances are easily identified by their main spectral features, which comprise strong sharp peaks.

SEM analysis

A more careful observation of explosive residues on the surface of the SERS substrate has shown that they tend to occupy the individual pits, not covering the surface of the substrate in a homogeneous way but rather completely occupying single sites randomly. In Figure 11, two SEM images of the SERS substrate: the first, acquired in the area covered by the deposited solution at low magnification (reference bar 10 nm, magnification 5000), shows traces of the explosive residues (in this case RDX) filling some pyramidal pits over a large area of the sample; the second, at higher magnification (reference bar 200 nm, magnification ~1.1·10^5) shows details of some pits full of explosive.
Through the analysis of Figure 11-a and similar by using the image processing and analysis software “ImageJ”, the explosive sampled resulted to be about 155 pg

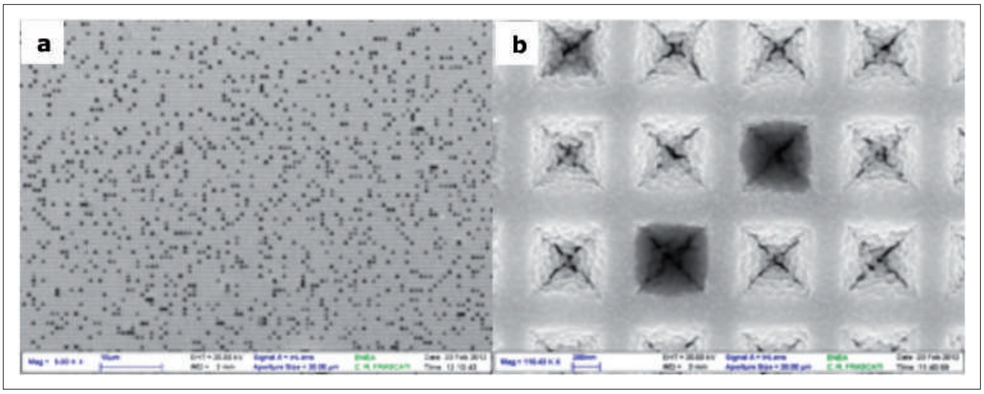


FIGURE 11 SEM images of the same SERS substrate at different magnification: (left) a large area randomly filled with the residual explosive (RDX); (right) a more detailed image of some filled pits

($155\cdot10^{-12}$ g). A similar procedure was applied for the other explosives, obtaining comparable quantities (about 200 pg).

Conclusions

The Raman techniques in both RADEX and SERS devices have demonstrated to supply valid and valuable results to the detection of very low trace level of sensitive materials.

In particular, RADEX was able to detect trace amounts of energetic materials using an eye-safe single pulse laser. The detection limit depends on the type of substance (i.e., on the Raman scattering cross section, the resonance frequency, and the stability of the molecules when excited with a 266 nm wavelength).

Detection of low surface densities, in the order of 100-1000 μg/cm^2, was obtained for the analyzed energetic materials respecting the constraint of a single laser pulse with 3 mJ/cm^2. RADEX seemed to be a robust apparatus since it was able to work inside a challenging environment, such as a metro station, without encountering any type of interference (i.e., dust, temperature, electromagnetic fields, humidity etc.).

Furthermore, SERS was used to detect explosives in quantities of about 150-200 pg. The high signal-to-noise of the spectra suggests the identification of the explosives could be clearly performed by their characteristic Raman spectra even at such low and, possibly, lower quantities. Spectra have been obtained non-destructively with a 10 s acquisition and 180 mW excitation, for a total fluence of $11.7\cdot10^3$ J/cm^2.

Both devices have opened a new possibility to increase the limit of detection of new threats not only for energetic materials but also for biohazards like deadly microorganisms that can be used in bioterrorist attacks.

Salvatore Almaviva, Federico Angelini, Roberto Chirico, Giovanni Dipoppa, Ivano Menicucci, Marcello Nuvoli, Adriana Puiu, Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation - Diagnostics and Laser Metrology Laboratory

Sabina Botti, Luciano Cantarini
ENEA, Technical Unit for the Development of Applications of Radiation - Photonics Micro and Nanostructures

Alessandro Rufoloni
ENEA, Technical Unit for Nuclear Fusion - Superconductivity Laboratory

references & notes

[1] B.M. Jenkins, B.R. Butterworth, 2010, MTI Report WP 09-02.
[2] Global terrorism database, 2013, National Consortium for the Study of Terrorism and Responses to Terrorism (START), http://www.start.umd.edu/gtd
[3] M. Marshall and J.C. Oxley, 2009, Elsevier, Oxford, ISBN: 978-0-12-374533-0.
[4] D.J. Gardiner, Practical Raman spectroscopy, 1989, Springer-Verlag, Amsterdam.
[5] S. Wallin, A. Pettersoon, H. Östmark, A. Hobro, 2009, in Anal. Bioanal. Chem., 395, 259-274.
[6] D.L. Jeanmaire, R.P. Van Duyne, 1977, "Surface Raman Spectroelectrochemistry Part I. Heterocyclic, Aromatic and Alipahtic Amines Adsorbed on the Anodized Silver Electrode", in J. Electroanal. Chem 84, 1-20.
[7] A. Otto, 1984, "Electronic Scattering. Spin Effects. SERS and Morphic Effects", in Ligth scattering in solids, vol 4, Springer, Berlin.
[8] M. Fleischmann, P.J. Hendra, A. J. McQuillan, 1974, "Raman Spectra of Pyridine Adsorbed at a Silver Electrode" in Chem. Phys. Lett., 26(2), 163–166.
[9] http://www.nato.int/cps/en/natolive/news_104536.htm
[10] E.C. Le Ru, E. Blackie, M.Meyer, P.G. Etchegoin, 2007, "SERS enhancement factors: a comprehensive study", in J. Phys. Chem. C, 111, 13794 – 13803.
[11] S. Efrima, H. Metiu, 1979, "Classical theory of light Scattering by an adsorbed molecule", in J. Chem. Phys., 70, 1602 - 1613.
[12] J. Gersten, A. Nitzan, 1980, "Electromagnetic theory of Enhanced Raman-scattering by molecules adsorbed on rough surfaces", in J. Chem. Phys., 73, 3023 – 3037.
[13] www.bonas-fp7.eu/
[14] A. Campion, J.E. Ivanecky, C.M. Child, M. Foster, 1995, "On the mechanism of chemical enhancement in surface-enhanced Raman scattering", in J. Am. Chem. Soc., 117, 11807-11808.
[15] W.E. Doering, S.M. Nie, 2002, "Single-molecule and single nanoparticle SERS: Examining the roles of surface active sites and chemical enhancement", in J. Phys. Chem. B, 106, 311-317.
[16] I.R. Lewis, N.W. Daniel, P.P. Griffiths, 1997, "Interpretation of Raman Spectra of Nitro-Containing explosives materials. Part I: group frequency and structural class membership", in App. Spect., 51(12), 1854-1867.
[17] Y.A. Gruzdkov, Y.M. Gupta, 2001,, "Vibrational Properties and Structure of Pentaerythritol Tetranitrate", in J. Phys. Chem. A, 105, 6197-6202.
[18] X. D. Gong, H.M. Xiao, 2001, "Studies on the molecular structure, vibrational spectra and thermodynamic properties of organic nitrate using density functional theory and ab initio methods", in Jou. Mol. Struct. (Theochem), 572, 213-221.
[19] D. Lin-Vien, N. B. Colthup, W.G. Fateley, J.G. Grasselli, 1991,The handbook of infrared and Raman characteristic frequencies of organic compound, John Wiley and Sons, New York.
[20] S. Almaviva, S. Botti, L. Cantarini, R. Fantoni, A. Palucci, A. Puiu, A. Rufoloni. 2013, "Trace level detection and identification of nitro-based explosives by Surface-Enhanced Raman Spectroscopy", in J. Raman Spectrosc., 44, 463-468.
[21] S. Almaviva, S. Botti, L. Cantarini, R. Fantoni, S. Lecci, A. Palucci, A. Puiu, A. Rufoloni, 2014, "Ultrasensitive RDX detection with Commercial SERS substrates", in J. Raman Spectrosc., 45, 41-46.

Rilevamento di precursori di esplosivi con tecnologia Lidar ad assorbimento differenziale mediante oscillatore parametrico ottico

Il presente studio è mirato allo sviluppo di un sensore laser remoto capace di rilevare i precursori utilizzati per fabbricare dispositivi esplosivi improvvisati (IEDs). Dopo uno studio spettroscopico preliminare in una cella di assorbimento, la fattibilità di un Lidar/DIAL (Differential Absorption Lidar) per il rilevamento di vapori di acetone è stata studiata in laboratorio, simulando le condizioni di campagne sperimentali sul campo. Infine, tenendo conto di misurazioni effettuate in uno scenario reale, è stato eseguito uno studio su eventuali interferenti atmosferici, ricercando tutti i composti noti che hanno in comune l'assorbimento nell'infrarosso (IR) dell'acetone nella banda spettrale selezionata per poterne rilevare la presenza. Possibili specie interferenti sono state studiate simulando sia un ambito urbano sia uno industriale: valori limite di rilevamento di acetone sono stati individuati in entrambi i casi. Lo studio qui descritto ha confermato che un Lidar/DIAL è in grado di rilevare acetone a bassa concentrazione anche a distanze notevoli.

Differential Absorption Lidar detection of explosive precursors by Optical Parametric Oscillator laser systems

The present study is aimed at the development of a laser remote sensor able to detect precursors employed in the manufacturing of IEDs (Improvised Explosive Devices). After a preliminary spectroscopic study in an absorption cell, the feasibility of a lidar/DIAL (Differential Absorption Lidar) for the detection of acetone vapors has been investigated in laboratory, simulating the experimental conditions of a field campaign. Eventually, having in mind measurements in a real scenario, a study of possible atmospheric interferents has been performed, looking for all known compounds that share with acetone infrared (IR) absorption in the spectral band selected for its detection. Possible interfering species were investigated simulating both urban and industrial atmospheres, and limits of acetone detection in both environments were identified. This study confirmed that a lidar/DIAL can detect low-concentration acetone at considerable distances.

DOI: 10.12910/EAI2014-89

■ *A. Puiu, L. Fiorani, R. Borelli, M. Pistilli, O. Rosa, A. Palucci*

Introduction

Terrorist bombings in the last few years led to an increased demand for the development of new technologies able to prevent such events. In particular,

■ **Contact person: Luca Fiorani**
luca.fiorani@enea.it

FIGURE 1 On 22nd July, 2011, the government buildings in Oslo were bombed (left picture) [livinginphilistia.blogspot.it], resulting in eight casualties. The bomb was made in a farmhouse (top right picture) [lionheartuk.blogspot.it] from fertilizer (bottom-right picture) [news.images.itv.com] and other explosive precursors

a remote sensor could have detected explosive precursors escaping from the farmhouse where the Oslo bombing was prepared (Fig. 1). Prevention means rapid identification of illegal bomb factories employed to produce IEDs, often based on triacetone triperoxide (TATP). Nowadays, this is possible thanks to the emerging remote sensing technologies based on recently developed laser sources.

In this work we report on acetone detection by means of a lidar/DIAL based on an Optical Parametric Oscillator (OPO) laser system, in the framework of the project BONAS (BOmb factory detection by Networks of Advanced Sensors). We used the "IR Opolette HE 3034" model by Opotek, that has the benefit of being a portable compact laser source tunable in the range 3 – 3.45 μm, where both TATP and its precursor acetone have quite strong absorption peaks. TATP ($C_9H_{18}O_6$) is a powerful explosive, easy to make using commonly available chemicals, such as acetone (C_3H_6O) and hydrogen peroxide (H_2O_2). Being not difficult to synthesize, TATP is often the explosive of choice for terrorists [1].

TATP is one of the most dangerous explosives known, being extremely sensitive to impact, temperature change and friction. Just a few hundred grams of the material produce hundreds of liters of gas in a fraction of a second [2]. Thus, the development of sensing systems able to identify illegal factories where IED are produced turns out to be of critical importance for the security of people and territory. The present research is focused on the remote detection of acetone, which can be identified in its vapor state outside the building where TATP is prepared.

Spectroscopy of acetone

Acetone (molecular weight: 58.0791 g mol^{-1}) is a colorless liquid, flammable and irritant with a high vapor pressure (24,600 Pa at 20 °C) [3]. Absorption spectra of acetone and TATP measured by Diffuse Reflectance Infrared Fourier Transform (DRIFT) spectroscopy [4] put in evidence that both substances exhibit many absorption peaks in the spectral interval from 3 to 10 μm.

Acetone has a few stronger absorption bands around 5.8 μm (C=O stretch), 7.3 μm, 8.2 μm (skeletal vibrations) and 18.85 μm, as well as weaker absorption bands at 3.4 μm (C–H stretch), 6.97 μm, 9.1 μm and 11.2 μm.

This is not surprising because generally, in an infrared (IR) spectrum, the less polar C–H bond has smaller absorption intensity than the more polar C=O bond. The region from 6.5 to 20 μm – called the 'fingerprint region' – usually contains a very complicated series of absorptions which are mainly due to all manner of bending vibrations within the molecule. It is much more difficult to pick out individual bonds in this region than it is in the clearer region at lower wavelengths (under 6.5 μm). In lidar atmospheric sensing, it is important to take into account not only the spectroscopic features of the species to be revealed, but also the spectroscopy of the atmosphere. For this reason, we performed transmittance simulations of acetone vapor, based on "The NIST Chemistry WebBook" [3, 5] and atmosphere, based on the "U.S. Standard Atmosphere, 1976" [6]. This study showed that the most intense absorption bands of acetone, free of atmosphere interference, are centered at 3.4 μm and 8.2 μm.

The spectral range below 2.5 μm was not considered in this simulation because it is characterized only by weak overtone bands of acetone. The 2.5 – 3 μm and 5 – 7.5 μm spectral windows are dominated by water, while the 4.1 – 4.5 μm band is completely covered by a strong carbon dioxide absorption and has no acetone spectral features. The 'fingerprint region' is considered an important spectral window because each different compound produces a different pattern of troughs in this particular region of the IR spectrum. The only problem to reveal acetone in the fingerprint region is its possible interference with other components of the atmosphere. In fact, at wavelengths longer than 14 μm, gases such as CO_2 and CH_4 (along with less abundant hydrocarbons) absorb strongly due to the presence of relatively long C–H and carbonyl bonds, as well as water vapor, that absorbs in rotation modes. As a consequence, acetone could potentially be detected using a lidar/DIAL system at wavelengths near 3.4 μm, 8.2 μm, 9.15 μm and 11.15 μm. Yet, in a real scenario we must consider that the presence of the IR radiation background may have a negative effect on the signal-to-noise ratio (SNR) of the instrument. The main contributions to IR background come from down-going solar radiation (IR energy coming from the Sun) and from up-going thermal radiation (IR energy coming from the Earth). By computing radiative transfer in the Earth's atmosphere with SBDART WebTool [7] it can be noticed the IR background is higher at longer wavelength. Taking into account the above spectroscopic considerations (related to atmosphere, acetone, IR background) and the requirement for a compact tunable unit with high pulse energy (> 3 mJ) and good beam quality (linewidth < 10 cm^{-1}), OPO turns out to be the proper light source for lidar detection of acetone. The OPO manufactured by Opotek has been chosen because of its ease of use, operational reliability, small volume and low weight. Nowadays, due to the development of the quantum cascade laser (QCL) technology [8], compact tunable laser sources working at room temperature are available from 2.75 μm to 16 μm, but the emitted energy is still too low for long-range remote sensing.

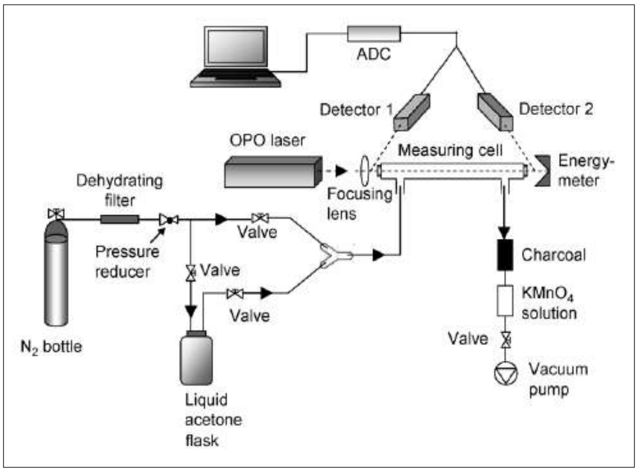


FIGURE 2 Table top set-up for spectroscopic measurements. ADC: analog-to-digital converter. The detectors are very sensitive and were illuminated by the small amount of radiation scattered by focusing lens (detector 1) and energy meter (detector 2), and no beam-splitter was used

Experimental set-up for in-cell acetone detection

In order to measure the transmission spectrum of vapor phase acetone at OPO emission wavelength, a table top experimental set-up was realized in our laboratory (Fig. 2). A glass cell (1.5 m long) closed by two ZnSe windows was filled with different concentrations of acetone. The vapors, produced in the flask containing pure liquid acetone (99.98% by Carlo Erba) at room temperature, were transported by a nitrogen flux into the measuring cell. The laser beam was slightly focused into the cell by a ZnSe lens and dumped on the energy-meter. The transmittance of the cell was measured by two detectors placed before and after the cell. At the cell exit, charcoal and/or $KMnO_4$ solution were introduced for safety reasons, to reduce the vapor

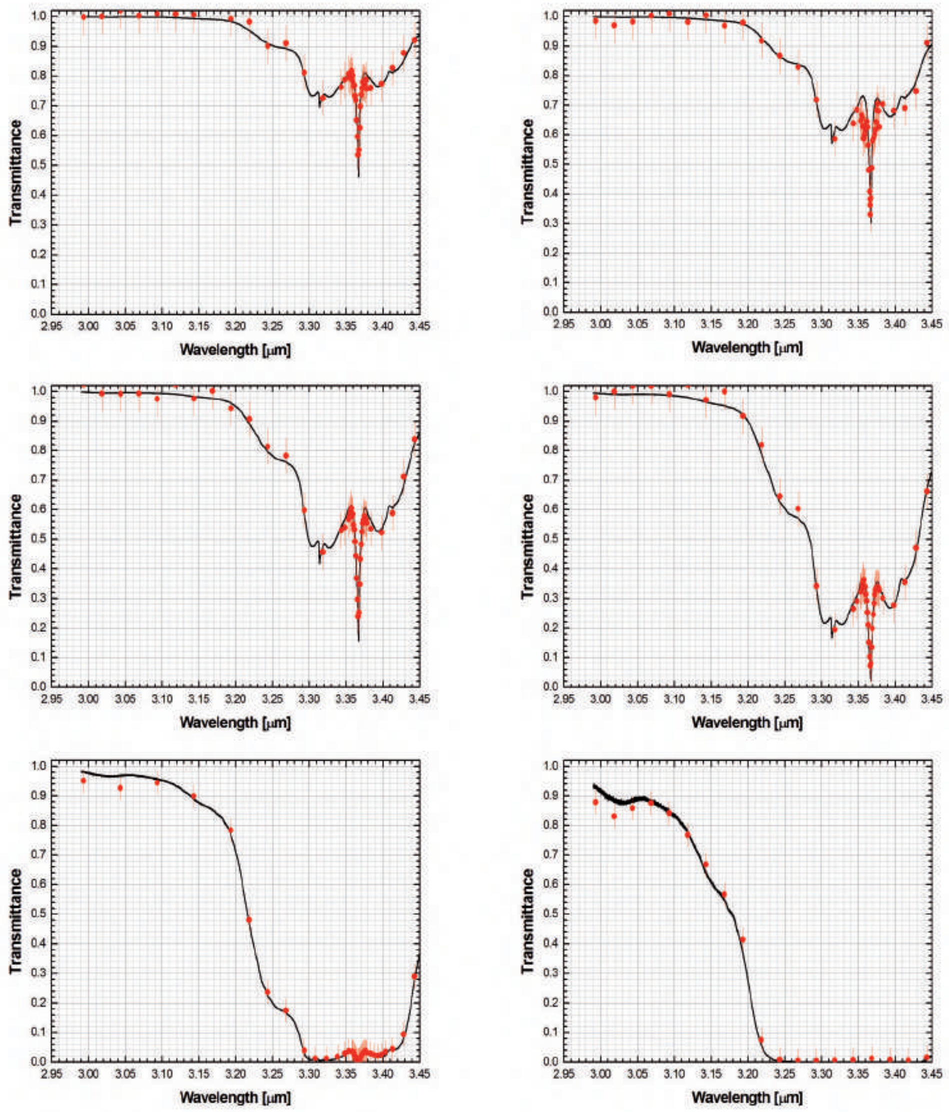


FIGURE 3 Transmittance of acetone measured at ENEA (dots) and according to the PNNL database (line) for six different concentrations: 1700 ppm (top left), 2600 ppm (top right), 3800 ppm (middle left), 8000 ppm (middle right), 25,000 ppm (bottom left) and 100,000 ppm (bottom right)

emissions of the explosive precursor under study.

The transmittance at a given wavelength has been obtained averaging 100 laser shots. Only a small part of the laser energy was used for the cell measurements (the OPO is equipped with a variable attenuator). The measured spectra were compared in Figure 3 with the Pacific Northwest National Laboratory (PNNL) database [10], that is more recent and has finer resolution with respect to the database [5] available in "The NIST Chemistry WebBook" [3].

The agreement between experimental measurement and PNNL data is good, especially for low transmittance. This is not surprising: high transmittance corresponds to small differences between the signal before and after the cell, more sensitive to the noise. The OPO by Opotek proved to be not only light-weight and compact, but also user-friendly and reliable. This makes the integration of this OPO laser into a portable lidar system possible. All these results confirm that OPO sources are good candidates for lidar/DIAL detection of IED precursors in real scenarios.

Lidar/DIAL measurements

A typical lidar system uses a laser to propagate a light pulse to a transparent or hard target. A fraction of the back-scattered light is collected by a telescope and focused onto a detector. The signal from the detector is then analyzed with the aid of high speed electronics to give information about the investigated atmosphere. A schematic of our lidar configuration is shown in Figure 4. Pump laser and OPO are integrated into a single compact unit, which is cooled by closed cycle water. The laser is a flash lamp pumped Nd:YAG emitting 1064 nm radiation with a pulse repetition rate of 20 Hz, a pulse length of 7 ns and a beam diameter of 4 mm. The OPO system has a maximum pulse energy of 3.4 mJ. The OPO beam characteristics – full angle divergence, waist beam size and beam quality factor – as measured in our lab, are reported in Table 1.

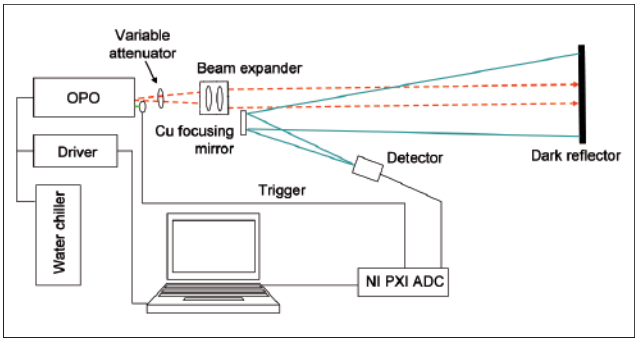


FIGURE 4 Schematic set-up of the laboratory OPO-lidar system. NI: National Instruments, PXI: PCI (Peripheral Component Interconnect) extensions for instrumentation. The trigger signal is provided by a photodiode observing the Nd:YAG pulse

In order to avoid detector saturation, we placed a variable attenuator on the beam path. The beam expander was used in order to match the transmitter divergence with the receiver field of view, as well as for eye safety reasons. In fact, according to the Directive 2006/25/EC of the European Parliament, for the following conditions:

a) laser exposure to the eye less than 10 s,
b) laser pulse duration from 1 to 100 ns,
c) wavelength range from 2.6 to 1000 μm,

the maximum permissible exposure MPE is 100 J/m^2. Having in mind that a typical laser footprint is about 1 cm^2, the maximum energy dose is around 10 mJ. If more than three shots of our system at its maximum energy are fired in one direction, the laser footprint has to be enlarged accordingly, and this can be easily accomplished by using a beam expander: at its output the diameter of the laser spot is about 1.2 cm, corresponding to 1 cm^2.

The lidar specifications are summarized in Table 2.

Laser parameter	Full angle divergence θ (mrad)	Waist beam size D_0 (mm)	Beam quality factor M^2
Horizontal	8.7	0.47	1.004
Vertical	6.0	0.68	1.005

TABLE 1 Laser beam features

Subsystem	Characteristics	
Transmitter (“IR Opolette HE 3034” model by Opotek)	Wavelength Attenuated pulse energy Pulse duration Pulse repetition rate	3362 nm 0.15 mJ 10 ns 20 Hz
Cu focusing mirror (manufactured in our lab)	Diameter Focal length	8 mm 197.5 mm
Detector (“PVI-4TE-3.4” model by Vigo)	Size Detectivity	1×1 mm^2 9.2×10^{11} cm $Hz^{1/2}$/W
ADC (“PXIe-5122” model by NI)	Sampling frequency Vertical resolution	100 MS/s 14 bit

TABLE 2 Specifications of OPO-lidar system

Laboratory tests for lidar/DIAL detection of acetone vapors

The laboratory tests were performed in order to assess the acetone concentration that could be found close to a window or an aeration duct of an illegal IED factory. For this, liquid acetone was placed in an uncovered glass Petri dish (diameter: 0.2 m) just below the laser beam, so the released vapor intercepted the laser beam.

The measurements were carried out in the following laboratory conditions: temperature T = 294.45 K; pressure P = 98,200 Pa; optical path ΔR = 0.2 or 6.35 m. The values 0.2 and 6.35 m correspond to the measurements carried out just after pouring acetone into the dish and waiting it to diffuse in the whole room, respectively. In fact:

- just after pouring acetone, we can assume that its vapors are present just over the Petri dish, i.e. in an optical path of 0.2 m;
- once acetone is diffused in the room, its vapors are distributed in all the optical path between transmitter and reflector (their distance is 6.35 m).

By applying to the Lambert-Beer law the records for acetone given by the PNNL database (acetone concentration $N_{ac} = 10^{-6}$ atm; optical path L = 100 cm, acetone absorbance at 3362 nm $A = 8.59\times10^{-7}$), and knowing the number of molecules of the standard atmosphere $N_{atm} = 2.46\times10^{-19}$ molecule/cm^3, the acetone cross section (σ) at 3362 nm was calculated to be 3.49×10^{-22} cm^2/molecule.

The first measurement (data1) was performed out just after pouring acetone while data2 – data4 were temporally spaced by a few minutes interval between them. The calculated acetone concentrations for the sequence of four acquisitions are reported in Table 3.

Knowing that the acetone diffusion coefficient in the air is 0.124 cm^2/s, we can assume that a short time after [data2], [data3] and [data4] were acquired, acetone diffusion covered all the range ΔR = 635 cm. As one can expect, the concentration of data1 is close to the acetone vapor pressure (246,000 ppm), while the average concentration in the room grows over time (data2 to data4).

Considering the case of a vapor plume near a bomb factory, it is reasonable to assume that the concentration is between 1 and 10%, i.e. we expect to find values of acetone concentration on the field between 2460 and 24,600 ppm. As can be noticed, the laboratory tests confirm that our OPO lidar system is a good candidate

Test data	Range ΔR [cm]	Measurement-derived acetone concentration [molecule/cm^3]	Measurement-derived acetone concentration [ppm]
[data1]	20	5.8×10^{18}	240,660
[data2]	635	4.3×10^{17}	17,842
[data3]	635	5.4×10^{17}	22,407
[data4]	635	6.9×10^{17}	28,630

TABLE 3 Results of laboratory test for lidar/DIAL detection of acetone vapor

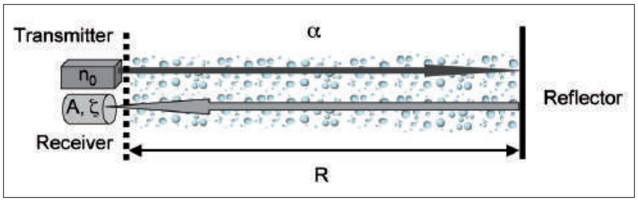


FIGURE 5 Lidar principle of operation in the presence of a hard target

for detecting such quantities of acetone. From the lidar equation [9] we can conclude that using a 300-mm telescope and removing the OPO attenuator (3 mJ instead of 0.15 mJ) 200 ppm of acetone should be detected at 1.5 km.

Received power and signal to noise ratio

In general, the backscattered lidar returns from a hard target are about six orders of magnitude higher than that from aerosols in the atmosphere. In the following, we shall consider the case of a hard target experiment (Fig. 5).

As a reflector (target) we used a rough dark surface of SBR (Styrene-Butadyene Rubber) composite. Usually, not all rough surfaces are Lambertian reflectors, but this is often a good approximation when the characteristics of the surface are unknown. If we consider a Lambertian surface where the target area is greater than or equal to the beamwidth and the receiver field of view is greater than or equal to the transmitter beamwidth [11], the lidar signal or power received or backscattered from a hard target (P_r) may be described by the Lidar Equation [9], [26], [27]. All the parameters used to calculate the received power for acetone detection with the experimental set-up described in Figure 4 were reported elsewhere [26], [27]. With this parameters, the calculated number of the received photons n_r was 8.2 x 10^{14}. Knowing that the energy of a single photon is $E = hc/\lambda$, for n_r photons we obtain a received power P_r of 5 x 10^{-5} W. The measured received power is given by the ratio between the acetone signal S [V] and the product of detector transimpedance T [V/A] and current responsivity R_i [A/W] at the laser wavelength of 3362 nm. Taking into account that the recorded acetone signal was 1.12 V, the measured received power results to be 6 x 10^{-5} W, very close to the calculated value (5 x 10^{-5} W). The equation and parameters used for the calculation of SNR were previously reported [26], [27]. A very good SNR was obtained (1.68 x 10^6).

Study of possible atmospheric interfering molecules in real scenarios

In this section we shall analyze the molecules normally present in the atmosphere which may interfere with acetone detection. For this study, we have chosen as a reference the US standard atmosphere [6] due to the richness of available data furnished by different Institutions, such as EPA (US Environmental Protection Agency) [13] and CDIAC (Carbon Dioxide Information Analysis Center) [14]. For the research of reference spectra of the selected interfering molecules, HITRAN [12] and NIST (National Institute of Standards and Technology) [3] databases were used. The molecules which may interfere with acetone detection (see Table 4) were selected taking into account their absorption coefficients for each compound (at standard atmospheric concentrations).

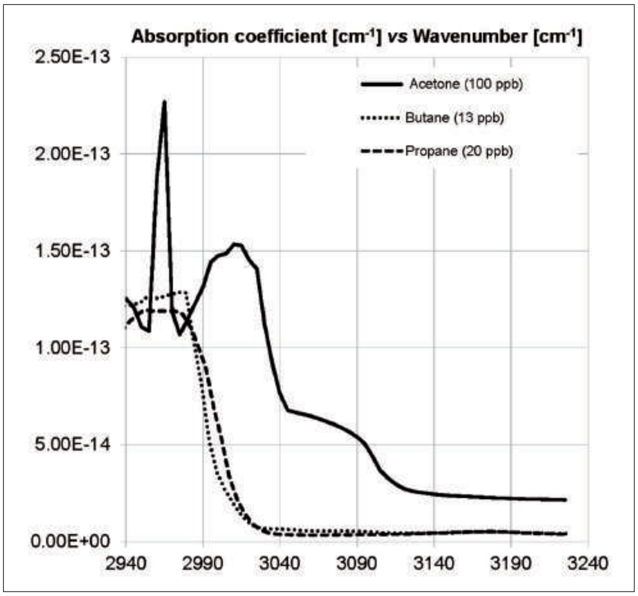


FIGURE 6 Simulation of molecular species interfering with 100 ppb of acetone in urban areas

Classes	Name	Formula	Database	Concentration (ppb)	Reference
Alkanes	Butane	C_4H_{10}	Nist	13.00	[15]
	Propane	C_3H_8	Nist	20.00	[15]
	Pentane	C_5H_{12}	Nist	0.207	[16]
Alkenes	1,3butadiene	C_4H_6	Nist	0.4	[17]
	Propene	C_3H_6	Nist	1.33	[18]
	Acetylene	C_2H_2	Nist	1.622	[18]
Alcohol	Isopropyl Alcohol	C_3H_8O	Nist	0.604	[18]
Epoxide	Ethylene Oxide	C_2H_4O	Nist	0.005	[19]
Aldehydes	Formaldehyde	C_2HO	Hitran	2.33	[20]
	Benzene	C_6H_6	Nist	0.22	[18]
Aromatic Hydrocarbons	Toluene	C_7H_8	Nist	0.42	[18]
	Strene	C_8H_8	Nist	0.1889	[21]
	Ethylbenzene	C_8H_{10}	Nist	0.05	[18]
Chloro Compounds	Chloromethane	CH_3Cl	Nist	0.7	[17]
	Dichloromethane	CH_2Cl_2	Nist	0.2	[17]
	Ethylene Dichloride	$C_2H_4Cl_2$	Nist	0.1	[17]
	Methyl Chloroform	$C_2H_3Cl_3$	Nist	0.113	[17]
	Chloroethene	C_2H_5Cl	Nist	$3.3x10^{-3}$	[22]
	Tetrachloro-ethylene	C_2Cl_4	Nist	0.1	[17]
	Tetrachloro-methane	CCl_4	Nist	0.13	[23]
	Chloroform	$CHCl_3$	Nist	0.1	[17]
Halons Compounds	Ethylene Dibromide	$C_2H_4Br_2$	Nist	0.02	[19]
	Methyl Iodine	CH_3I	Nist	0.002	[24]
Sulfur Compounds	Carbonyl Sulfite	OCS	Nist	0.466	[25]
	Carbon Disulfide	CS_2	Nist	0.038	[26]
Nitrogen Compounds	Nitrogen Dioxide	NO_2	Nist	11.44	[24]
	Ethyl Nitrate	$C_2H_5NO_3$	Nist	0.003	[20]

TABLE 4 List of selected interfering molecules

In Table 4 the compounds mostly cited in literature as present in the atmosphere at measurable levels are listed. From this study we excluded the pollutants having no spectral features in the wavelengths range covered by OPO, such as: sulfur dioxide (SF_6), bromotrifluoromethane ($CBrF_3$), chlorodifluoromethane ($CHClF_2$), dichlorofluoromethane (CCl_2F_2), fluoroform (CHF_3), bromoclorodiflouromethane (CF_2ClBr), 1-chloro 1,1- difluoroethane ($C_2H_3F_2Cl$), methyl bromide (CH_3Br), dichlorodifluoroethane ($C_2H_2Cl_2F_2$), and sulfur dioxide (SO_2).

Having in mind the considerations made so far, we shall examine the feasibility of a lidar/DIAL detection of acetone in different environments. Two scenarios (urban and industrial atmospheres) have been considered.

By simulating acetone in urban atmosphere (Fig. 6), we obtained that for acetone concentrations ≤100

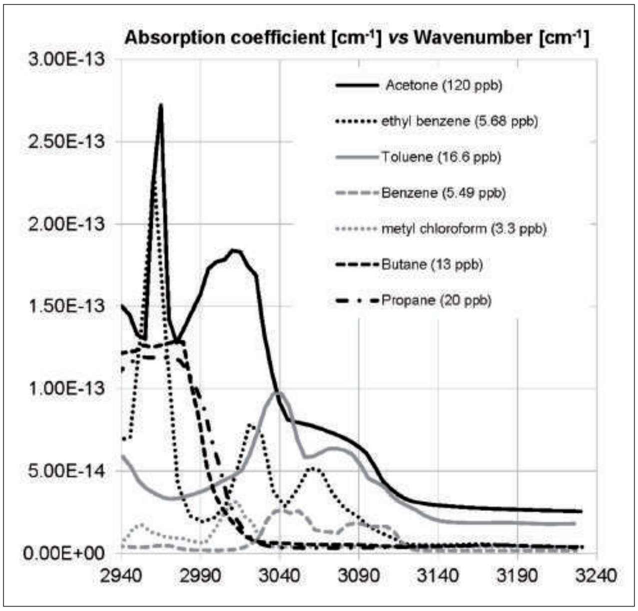


FIGURE 7 Simulation of molecular species interfering with 120 ppb of acetone in industrial areas

ppb, butane and propane absorption profiles start to interfere with acetone measurement.

If we suppose a scenario in which we have to measure acetone in a very polluted atmosphere, such as an industrial area, we found that ethyl-benzene and toluene start to interfere for acetone concentrations ≤120 ppb (Fig. 7), while butane and propane absorption remains unchanged.

In summary, in industrial areas, when dealing with an acetone concentration of about 120 ppb, we may find four main interfering species: butane, propane, ethyl-benzene and toluene; but this is not limitative since not all the spectral interval where OPO emits is covered by interfering species. In principle, by choosing two appropriate wavelengths (λ_{ON} ~ 3010 cm^{-1} and λ_{OFF} ~ 3145 cm^{-1}), a lidar/DIAL system can be employed to detect acetone in concentrations of the order of 100 ppb.

Conclusions

The aim of this work was to prove the capability of the developed lidar/DIAL system to measure precursors of IEDs, such as acetone nearby illegal factories. From the spectroscopic considerations on acetone, we may conclude that the best spectral bands for acetone detection are centered around 3.4 and 8 μm. The spectral interval from 3.1 to 3.45 μm, investigated with a laser having $\Delta\lambda \sim 10$ cm^{-1}, was chosen, as this spectral region is almost free from atmospheric interference and solar background. Laboratory tests were performed in order to monitor acetone with an OPO lidar/DIAL system. Results indicate that the measured signal coincide with the ones derived from the performed measurements by about 10%, and the detection limit is 200 ppm of acetone at a range of 1.5 km.

From the study of possible atmospheric interfering molecules in a real scenario, we can conclude that it is possible to measure acetone in both scenarios: urban and industrial environments till 120 ppb with no risk of false positive. Moreover, by using a compact laser source, the laboratory set-up can be easily integrated into a portable system for on-field measurements.

Acknowledgements

The support from the EU-FP7 BONAS project (contract no. 261685) is gratefully acknowledged.

Within the BONAS project a joint experimental test has been arranged at the AM-CSV (Italian Military Aeronautics - Experimental Flight Center) facility at Pratica di Mare airport, the logistic support and participation from AM personnel is kindly acknowledged.

Adriana Puiu, Luca Fiorani, Rodolfo Borelli,
Marco Pistilli, Olga Rosa*, Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation -
Diagnostics and Laser Metrology Laboratory
* guest student

references & notes

[1] I. Dunayevskiy, A. Tsekoun, M. Prasanna, R. Go, C.K.N. Patel, 2007, Appl. Opt,. 46, 6397.

[2] http://www.globalsecurity.org/military/systems/munitions/tatp.htm

[3] P.J. Linstrom, W.G. Mallard, 2001, J. Chem. Eng. Data, 46, 1059.

[4] A. Puiu, G. Giubileo, S. Nunziante Cesaro, 2012, Int. J. Spec., 953019.

[5] A.L. Smith, 1982, The Coblentz Society Desk Book of Infrared Spectra, Second Edition, The Coblentz Society Kirkwood US.

[6] U.S. Standard Atmosphere, 1976, United States Government Printing Office Washington, US.

[7] P. Ricchiazzi, S. Yang, C. Gautier, D. Sowle, 1998, Bull. Am. Met. Soc., 79, 2101.

[8] J. Faist, F. Capasso, D.L. Sivco, C. Sirtori, A.L. Hutchinson, A.Y. Cho, 1994, Science, 264, 553.

[9] L. Fiorani, "Lidar application to litosphere, hydrosphere and atmosphere", 2010, in Progress in Laser and Electro-Optics Research, V.V. Koslovskiy, ed. 21-75 Nova, New York US.

[10] S.W. Sharpe, T.J. Johnson, R.L. Sams, P.M. Chu, G.C. Rhoderick, P.A. Johnson, 2004, Appl. Spectrosc., 58, 1452.

[11] G. Mamon, D.G. Youmans, Z.G. Sztankay, C.E. Mongan, 1978, Appl. Opt., 17, 205.

[12] L.S. Rothman, I.E. Gordon, A. Barbe, D.C. Benner, P.F. Bernath, M. Birk, V. Boudon, L.R. Brown, A. Campargue, J.P. Champion, K. Chance, L.H. Coudert, V. Dana, V. M. Devi, S. Fally, J.M. Flaud, R.R. Gamache, A. Goldman, D. Jacquemart, I. Kleiner, N. Lacome, W.J. Lafferty, J.Y. Mandin, S.T. Massie, S.N. Mikhailenko, C.E. Miller, N. Moazzen-Ahmadi, O.V. Naumenko, A.V. Nikitin, J. Orphal, V.I. Perevalov, A. Perrin, A. Predoi-Cross, C.P. Rinsland, M. Rotger, M. Šimecková, M.A.H. Smith, K. Sung, S.A. Tashkun, J. Tennyson, R.A. Toth, A.C. Vandaele, J. Vander Auwera, 2009, J. Quant. Spectrosc. Radiat. Transfer, 110, 533.

[13] http://www.epa.gov/ttnemc01/ftir/welcome.html

[14] http://cdiac.ornl.gov/oceans/LDEO_Underway_Database/

[15] D.R. Worton, W.T. Sturges, C.E. Reeves, M.J. Newland, S.A. Penkett, E. Atlas, V. Stroud, K. Johnson, N. Schmidbauer, S. Solberg, J. Schwander, J.M. Barnola, 2012, Atmospheric Environment, 54, 592.

[16] Department of Environment and Natural Resources, Ambient Monitoring Section, 2009 Ambient Air Quality Report, State of North Carolina, Report # 2012.01, May 2012.

[17] Atmospheric Science Section of the Department of Environment and Conservation (NSW) of Australia, Ambient Air Quality Research Project 1996-2001, Internal working paper no. 2 "Ambient concentrations of toxic organic compounds in NSW".

[18] B. Zielinska, W. Goliff, 2003, Final Report Central California Ozone Study - Volatile Organic Compounds Collection and Analysis by the Canister and Tenax Methods, Division of Atmospheric Sciences Desert Research Institute.

[19] J.H. Seinfeld, S.N. Pandis, "Summary of the Average December 1977 Concentrations of Measured Trace Constituents Containing Halogens", in Atmospheric Chemistry and Physics: From Air Pollution to Climate Change, 1st Edition.

[20] O. Hawas, D. Hawker, D. Cohen, E. Christensen, G. Golding, P. Vowles, 2002, J. Chromatogr. A., 971, 173.

[21] J.H. Seinfeld, S.N. Pandis, 2006, Status of Toxic Air Contaminant Identification (California Air Resources Board, Atmospheric Chemistry and Physics: From Air Pollution to Climate Change, 2nd Edition).

[22] J.C. Low, N.Y. Wang, J. Williams, R.J. Cicerone, 2003, J. of Geophysical Research, 108, 4608.

[23] Initial Statement of Reasons for Proposed Rulemaking State of California (California Environment Protection Agency, Air Resources Board Staff Report, February 2009).

[24] N. Bell, L. Hsu, D.J. Jacob, M.G. Schultz, D.R. Blake, J.H. Butler, D.B. King, J.M. Lobert, and E. Maier-Reimer, 2002, J. Geophys. Res., Vol. 107, No. D17, DOI: 10.1029/2001JD001151

[25] P.J. Maroulis, A.L. Torres, A.R. Bandy, 1977, Geophys. Research Letters, 4, 510.

[26] P.J. Maroulis, A.L. Torres, A.R. Bandy, 1980, Geophys. Research Letters, 7, 681.

[27] L. Fiorani, A. Puiu, O. Rosa, A. Palucci, 2013, "Lidar/DIAL detection of bomb factories", in Proc. of SPIE, 8897, 889707-1.

Fluorosensore Lidar a scansione per il rilevamento in una scena post esplosione di detriti plastici derivanti da dispositivi esplosivi improvvisati

Il fluorosensore Lidar a scansione basato sulla fluorescenza indotta da laser (LIF) è stato applicato al fine di rilevare, in uno scenario post-esplosione, residui di plastico derivanti da dispositivi esplosivi improvvisati (IED). La sua capacità di misurazione in remoto, l'invasività minima, l'elevata sensibilità e l'applicabilità in loco rendono questo sistema molto promettente in campo forense per ottimizzare la raccolta di elementi probatori. Questa attività è stata sviluppata grazie al progetto FORLAB (FORensic LABoratory for in-situ evidence analysis in a post blast scenario), approvato e finanziato dalla Commissione Europea nell'ambito del Settimo programma quadro.

Scanning Lidar fluorosensor for detection in a post blast scene of plastic debris coming from Improvised Explosive Devices

The Scanning Lidar fluorosensor based on Laser Induced Fluorescence (LIF) has been applied for detection in a post blast scenario of plastic debris coming from Improvised Explosive Devices (IEDs). The advantages it offers of remote measurement capability, minimal invasiveness, high sensitivity, and in situ applicability make the system very promising in the forensic context to optimize the collection of evidences. This activity has been supported by the FORLAB project (FORensic LABoratory for in-situ evidence analysis in a post blast scenario), approved by the European Commission and funded under the FP7.

DOI: 10.12910/EAI2014-90

■ *L. Caneve, F. Colao, I. Menicucci, A. Palucci, M. Pistilli, V. Spizzichino, G. Terranova*

Introduction

In a post blast scene following an IED attack, the detection of evidences that can lead to a fast identification of the terrorist group or even the bomb maker (the IEDs components, such as explosive residues, electronic debris, or plastic or metal pieces of the container, shrapnel, etc.) is very important (Fig. 1). Sensors for fast screening of post-blast evidences, reducing the number of evidences sent to

■ **Contact person: Luisa Caneve**
luisa.caneve@enea.it

FIGURE 1 The crater caused by the explosion in the Capaci's massacre of magistrate Giovanni Falcone [May 23th 1992]. The arrow indicates the water canal into which the explosives have been inserted
Source: http://www.palermoplanet.it/html/mafia/digilander.libero.it/inmemoria/strage_capaci.htm#immagini

the reference forensic laboratory and the time of data acquisition, and increasing the information provided by the evidences left by the explosion during the investigations, are desirable.

In this respect, the EC considers of high strategic relevance contributing to the development of new technologies in support to forensic activities, through the Security Call instrument under the 7th Framework Programme 2007-2013.

The FORLAB project, funded by FP7 grant agreement no. 285052, aims at providing End Users with portable systems that will improve their efficiency in investigating the crime scene [1]. A schematic view of the project's approach is depicted in Figure 2.

An innovative LIF-based sensor has been developed and applied in the frame of the FORLAB Project for detection in a post blast scene of plastic debris coming from IEDs components.

The Laser Induced Fluorescence technique has been already used for cultural heritage protection and restoration activities [2,3,4], but the LIF sensor capability of rapid scanning of large areas at distances up to some tens of meters with high spatial resolution [5] makes this instrument very advantageous in security applications.

Among the spectroscopic techniques appropriate to remote application, the Fluorescence Induced upon ultraviolet Laser excitation is able to supply valuable information thanks to its characteristic to give information on substances having specific spectral signature [6].

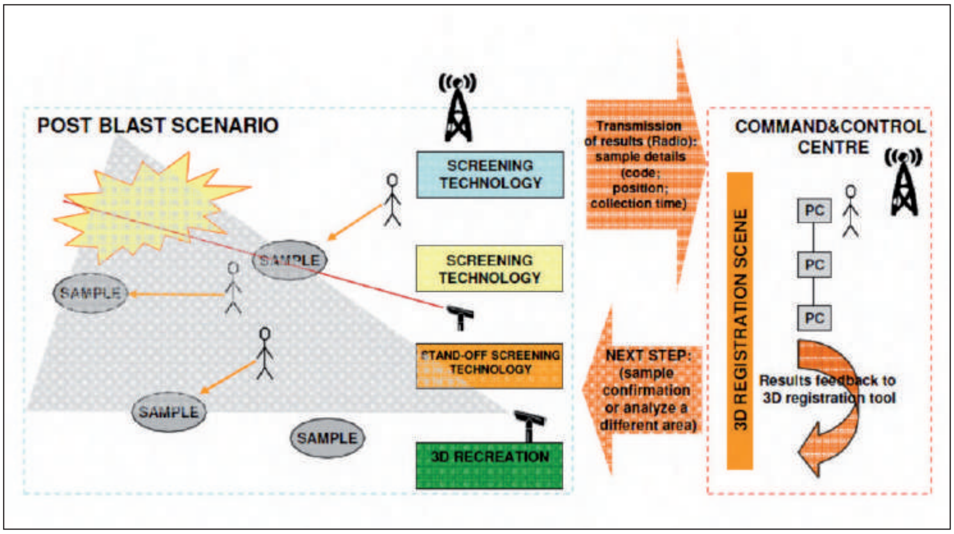


FIGURE 2 Operational diagram of the FORLAB project
Source: FORLAB Project Description of Work

In forensic applications, the additional capability of active reflectance measurements represents a significant step forward in the identification and precise localization of debris dispersed all around the crime scene.

Sophisticated data processing techniques – such as false-color imaging, principal component analysis (PCA) [7] on spectra, and spectral angle mapping (SAM)[8] on images – permit to detect and localize characteristics invisible to the naked eye[9].

LIF scanning system performances have been

FIGURE 3 LIF scanning system during in field campaigns in Bièvres (France) on January, 2013 and Wroclaw (Poland) on September, 2013

tested in real field conditions during different test campaigns (Fig. 3). The relevant results will be presented.

Experimental

The LIF technique is a molecular spectroscopy for surface analysis, based on the interaction of the ultraviolet radiation emitted by a laser with the matter[10]. The emission of radiation by luminescent materials is observed whenever an absorption of energy sufficient to activate the allowed electronic transitions occurs. In a typical LIF instrument, an ultraviolet (UV) laser beam irradiates a sample and an optical system collects and measures the emitted fluorescence signal. The spectral content of the radiation coming from the examined surface supplies information on the composition of the outer layers, once interrogated at different excitation wavelengths. It is a fast, non-invasive, remote, sensitive and selective technique.

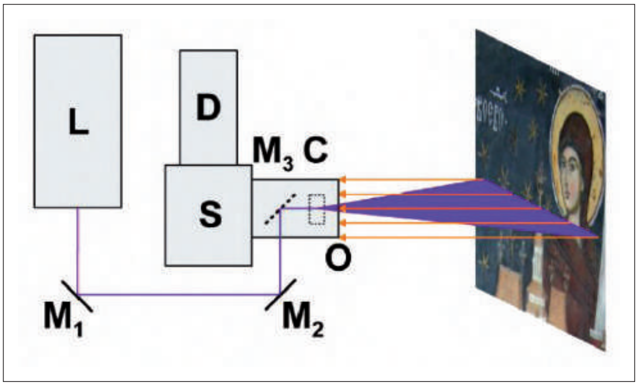


FIGURE 4 Schematic diagram of the ENEA LIF experimental set-up: L-laser, D-detector, S-spectrometer, M-mirrors, C-cylindrical lens, O-objective

A LIF scanning instrument (see Fig. 3), able to collect hyperspectral fluorescence images on large areas, has been realized at the ENEA's Diagnostic and Metrology laboratory in Frascati. The system has been developed with the aim of increasing the performances in terms of space resolution, time resolved capabilities and data acquisition speed with respect to the previous versions [11], by means of the line-by-line scanning process, particularly suitable for investigation on large areas. Its compact arrangement, reduced size and light weight allow for an easy transfer of the system. A typical experimental arrangement used for LIF is schematically depicted in Figure 4.

The optical system based on the use of a cylindrical lens, focusing the laser spot as a line, allows to scan an image of 1.5×5 m^2 in less than 2 minutes at 25 m. This arrangement is characterized by having the target spatial and spectral information on two mutually orthogonal directions imaged on the detector, with a sub-millimeter spatial resolution and a spectral resolution higher than 2 nm. Moreover, time resolved measurements on the nanosecond scale can be performed by controlling the electronic detector gate in a boxcar-like configuration. The collected data are released as false color reflectance and fluorescence images, suitable to the identification of original and added materials.

Each scan is controlled by a portable computer, where a specific program developed in LabView allows to set experimental parameters, control data acquisition, and perform a preliminary data analysis. Data are collected as both 2D monochromatic images and LIF spectra for each pixel. Additionally, the LIF scanning system can be utilized, with the laser switched off, to collect reflectance images upon the availability of an intense standard light source. When using a continuous light source like a lamp, the synchronism for data acquisition is given by the detector itself. Both fluorescence and reflectance images can be reconstructed in false colour by using the three most intense features detected, associated to Red, Green and Blue (RGB) channels, respectively.

Results

Preliminary laboratory measurements have been performed on some objects that can be actually found in a place invested by a blast – such as electronic debris, plastic materials, building fragments – to optimize the system characteristics and to obtain reference spectra. The results for some different target materials, also collected from a post blast scene, are reported in Figure 5. For these measurements, as well as for the

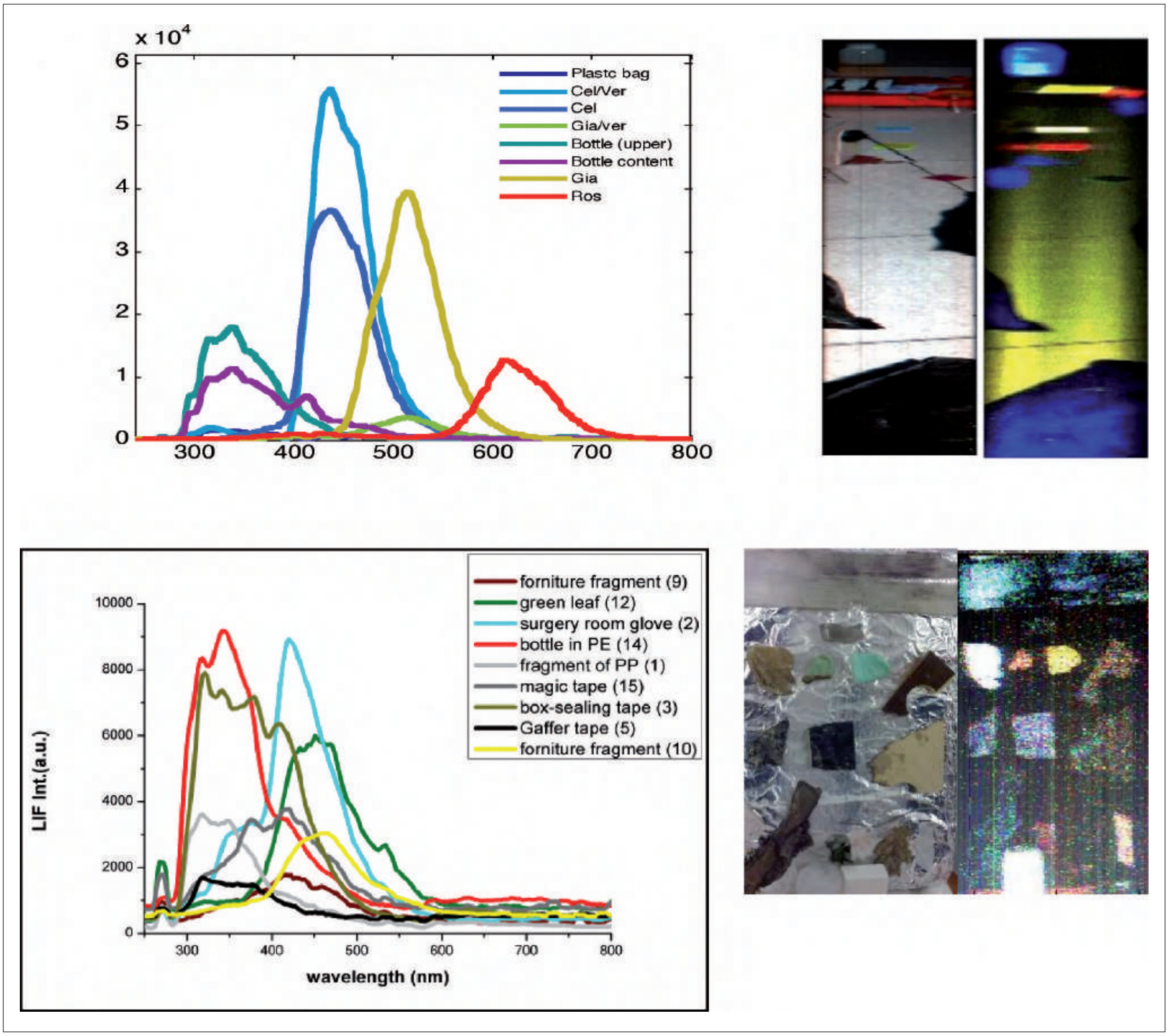


FIGURE 5 Laboratory test on different target materials, also collected from a post blast scene (below)

tests in Bièvres, the laser worked at 266 nm, with a pulse duration of 10 ns of and energy of 1.5 mJ. Distinct prevalent bands in the resulting fluorescence emission spectra have been identified depending on the target material. Fluorescence images have been obtained and the RGB false-color reconstruction has been performed by using the three most intense detected bands, the RGB channels. Conventional pictures are

FIGURE 6 Scenario in Bièvres test before (left) and after (right) the blast
Source: FORLAB LCCP Training

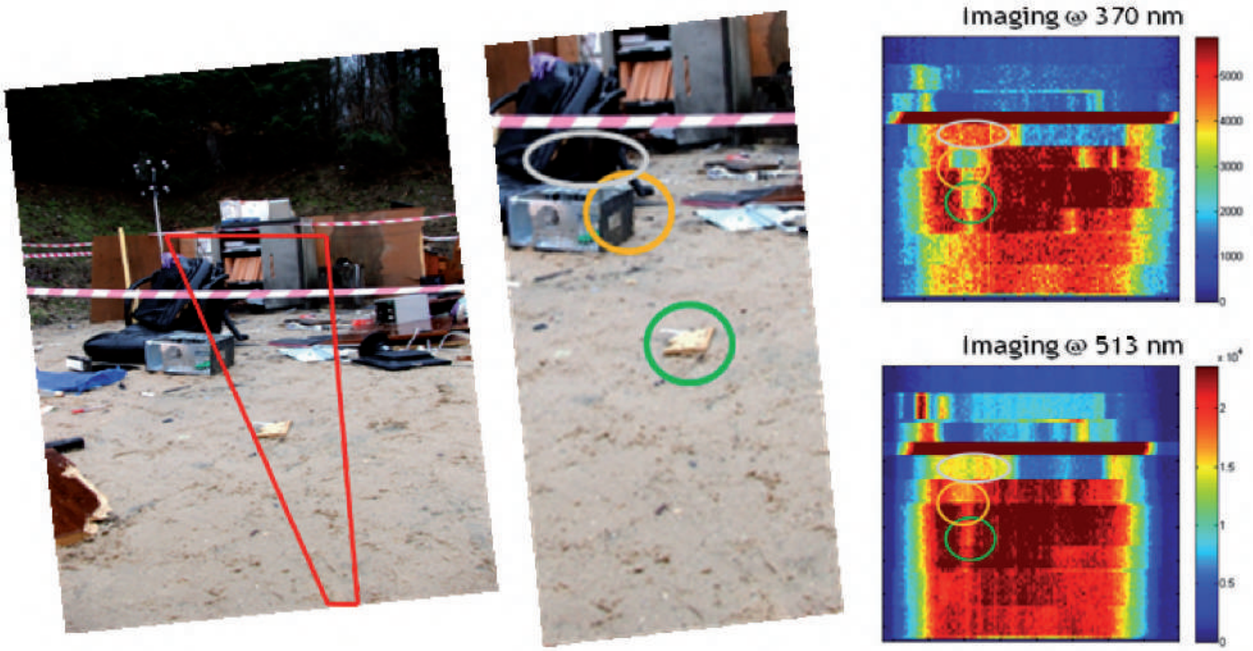


FIGURE 7 Fluorescence images by LIF system at two selected bands (370 nm and 513 nm)

FIGURE 8 Post-blast outdoor and indoor scenarios in Wroclaw's test

FIGURE 9 Fluorescence images of areas of the outdoor (left) and indoor (right) scenarios reconstructed by the RGB method

shown for comparison.

A first database of fluorescence spectra of materials that can be found in an IED has been created. Based on the reference spectra it was possible to identify plastic materials in real scenes reconstructed for in situ tests.

During the training test in Bièvres (Fig. 6), measurements on a post–blast scenario have been performed by the LIF scanning system. Fluorescence images have been obtained and by the analysis performed at different spectral bands, conveniently selected, some plastic debris have been evidenced on the scene.

In particular, fluorescence images at 370 nm and 513 nm (Fig. 7) have been analyzed and some different plastic debris individuated on the scene, circled in the figure, can be discriminated by their different spectral signature.

The second test campaign has been organized within the project to test the capabilities of the screening technologies developed in the first stage of the project and the integration level of all developed sub-systems. Main goal of the campaign in Wroclaw was testing the ability of the LIF system to identify plastic debris in complex environment, i.e. that of a typical post-blast site contaminated by debris and shrapnel of any sort of shape and origin. Two indoor and outdoor environments were simulated, since materials mixed with IED remains were different: fragments of furniture, appliances and paper for the first scenario (indoor), fragments of buildings, plants and cars in the second scenario (outdoor) (Fig. 8). Furthermore, distances, light conditions, and spaces were also very dissimilar. The outdoor scenario, for example, has been investigated looking at the area in the explosion site at a 4-to-15-meter distance, with a field of view of 6 degrees. Several scans were run and the corresponding fluorescence images were acquired. Images acquired in outdoor and indoor environments are shown in Figure 9. The conventional photograph and a red frame indicating the portion scanned with the LIF sensor are reported. The corresponding fluorescence image is reported as well, where several polymeric debris are clearly visible. The system high spatial resolution allows to detect debris of average size less than 1 centimeter.

As far as the latter is concerned, the RGB technique was used for rendering to enhance specific spectral signature and allow the discrimination among different polymeric materials.

Conclusions

The LIF scanning system has shown, in conclusion, its ability in obtaining valuable information on the presence and distribution of evidences of different materials on large areas.

The possibility to identify by the system small single debris out of a very crowded and confusing area commonly found in post-blast scenarios has been verified.

Tests on post-blast scenes have demonstrated the ability of the system to discriminate plastics from other materials, and among plastics for an effective discrimination of materials that can be used for an IED preparation. Easy-to-read spectral images have been produced with short acquisition times both in laboratory conditions and in situ.

The capability of remote material identification by means of the available data processing methods on raw hyperspectral images has been demonstrated.

Luisa Caneve, Francesco Colao, Ivano Menicucci,
Antonio Palucci, Marco Pistilli, Valeria Spizzichino
ENEA, Technical Unit for the Development of Applications of Radiation - Diagnostics and Laser Metrology Laboratory

Gaetano Terranova
ENEA, Technical Unit for the Development of Applications of Radiation - Photonics Micro and Nanostructures

references & notes

[1] http://www.fp7-forlab.eu/

[2] D. Anglos, M. Solomidou, I. Zergioti, V. Zaffiropulos, T.G. Papazoglou, C. Fotakis, 1996, “Laser-induced fluorescence in artwork diagnostics: an application in pigment analysis”, in Applied Spectroscopy, 50, 1331-1334.

[3] A. Nevin, G. Spoto, D. Anglos, 2012, “Laser spectroscopies for elemental and molecular analysis in art and archaeology”, in Appl. Phys. A, 106, 339-361.

[4] R. Grönlund, S. Svanberg, J. Hällström, K. Barup, G. Cecchi, V. Raimondi, D. Lognoli, L. Palombi, 2007, “Laser-induced fluorescence imaging for cultural heritage”, in Proc. of SPIE 6618, 66180P-1 66180P-8.

[5] L. Caneve, F. Colao, R. Fantoni, L. Fiorani, 2013, “Scanning lidar fluorosensor for remote diagnostic of surfaces”, in Nuclear Instruments & Methods In Physics Research A, 720, 164-167.

[6] A. Nevin, D. Anglos, 2006, “Assisted interpretation of laser-induced fluorescence spectra of egg-based binding media using total emission fluorescence spectroscopy”, in Laser Chemistry 01/2006; DOI: 10.1155/2006/82823

[7] K.V. Mardia, J.M. Kent, 1979, Multivariate Analysis, Academic Press, London.

[8] G. Girouard, A. Bannari, A. El Harti and A. Desrochers, 2004, “Validated Spectral Angle Mapper Algorithm for Geological Mapping: Comparative Study between Quickbird and Landsat-TM”, presented at the XXth ISPRS Congress, Geo-Imagery Bridging Continents, Istanbul, Turkey, 12–23 July 2004.

[9] D. Lognoli, G. Cecchi, I. Mochi, L. Pantani, V. Raimondi, R. Chiari, T. Johansson, P. Weibring, H. Edner, T. Svanberg, 2003, “Fluorescence lidar imaging of the cathedral and baptistery of Parma”, in Appl. Phys. B 76, 457-465.

[10] J.L. Kinsey, 1977, “Laser-Induced Fluorescence”, in Annual Reviews Physical Chemistry, 28, 349-372

[11] F. Colao, L. Caneve, A. Palucci, R. Fantoni, L. Fiorani, 2008, “Scanning hyperspectral lidar fluorosensor for fresco diagnostics in laboratory and field campaigns” in J. Ruiz, R. Radvan, M. Oujja, M. Castillejo, P. Moreno (Eds.) Lasers in the Conservation of Artworks 149-155.

Dispositivi innovativi per agenti biologici e contaminanti alimentari

Il rilevamento di agenti biologici pericolosi necessita di strumenti che ne consentano un'identificazione tempestiva e accurata. In tale contesto, la spettroscopia Raman/SERS e la fotoacustica rappresentano strumenti rapidi e sensibili di monitoraggio e identificazione sia di agenti patogeni nell'ambiente e nel cibo, sia di sofisticazioni alimentari. Nel quadro della sicurezza ambientale e alimentare, si descrivono due nuovi sensori messi a punto per il rilevamento di agenti chimici e biologici nocivi per la salute.

Innovative devices for biohazards and food contaminants

The detection of dangerous biological agents requires tools that allow their early and accurate identification. In this context Raman/SERS and photoacoustics techniques represent fast and sensitive tools for monitoring and identifying both pathogens in the environment and food, and sophistication in food.
In the framework of environmental and food security, two new sensors are described, developed for the detection of biological and chemical agents dangerous for health.

DOI: 10.12910/EAI2014-91

■ *A. Lai, S. Almaviva, V. Spizzichino, L. Addari, G. Giubileo, G. Dipoppa, A. Palucci*

Introduction

Despite the long history of nations and people using bacteria agents as weapons [1, 2], and the use of Salmonella in 1984 for poisoning food in salad bars in Oregon, it is only in the last decade that biological weapons have received attention to a greater extent [3]. In fact in 2001 intentional release of endospores of *Bacillus anthracis* caused 19 infections, 5 deaths and 10 000 prescriptions of antibiosis (Center for Disease Control and Prevention 2002).

The endospore is a quiescent, rough, and non-reproductive structure (endurance forms) produced by bacteria in response of adverse environment conditions as well as lack of nutrients [4]. Thanks to their resistance to heat, radiation and desiccation, [5] the endospores can survive for many years, as long as the environmental conditions return good for germination and vegetative cells development [6, 7]. The genus Bacillus includes species endospore–forming as *B. anthracis*, that are important for health because of their capability to produce exo-toxins, the virulence factors, after germination. The characteristics of survival and resistance make endospores the ideal delivery vehicles for their distribution into the environment. The range of lethal dose of *B. anthracis* is from 500 to 55,000 inhaled spores [8], and the antibiosis treatments must begin within a day or two of inhalation [9].

The borderline between bioterroristic materials and contaminants, additives or better adulterants in goods and food is very narrow to rise the alarm also to everyday market consumers (e.g., botulinum toxin in canned foods). In fact, many examples are present in the market distribution chain as some specific adulterating substances like melamine, methanol, aspartame and ammonia, just to report the

■ **Contact person: Antonia Lai**
antonia.lai@enea.it

most famous. The adulterants to be detected by new sensors have been selected due to their presence in very common goods present daily on our tables, such as extra virgin oil, methanol, powder milk, fresh fish. In this respect, in EU countries regulations on production, manipulation, and distribution stages are very severe, especially in Italy [10].

In this context accurate, fast, and relatively simple methods of analysis to be implemented in early detection of suspicious materials (e.g., biohazards or contaminants) is essential to ward off disease outbreak and dispersion in the environment.

The Diagnostic and Metrology (DIM) Laboratory has contributed to the development of new monitoring tools with its background in spectroscopy field, in both EU and national projects.

Raman spectroscopy, and in particular the Surface Enhanced Raman Spectroscopy (SERS) technique, has recently attracted attention on homeland security for the capability in the identification and detection of microbes and bioagents (small particle detection). In this context, the DIM Laboratory is partner of the project "Rapid-Air Monitoring particle against Biological threats" (RAMBO) in the framework of the European Defense Agency (EDA) Joint Investment Program on Chemical, Biological, Radiological and Nuclear protection (CBRN protection). Main aim of this project is to develop an advanced combination of two sensors, a Raman technique devoted to the first alarm and the Polymerase Chain Reaction (PCR) to confirm the suspicious biological threats. It is expected to have high performances (towards the one spore limit), high selectivity, rapid response (<45 minutes), portability.

Conversely, the Laser PhotoAcoustic Spectroscopy (LPAS) has been implemented in the frame of the National Project SAL@CQO with the main aim of developing and applying innovative, easy-to-use product-instruments to be used by stakeholders or regulatory authorities in production chains, where food processing requires the continuous monitoring of quality and preservation of food included in the process.

Both Raman and LPAS offer the advantages to analyze samples without preparation, in real time, on line, and also in the remote mode.

Materials and methods

Biohazard measurement have been performed with

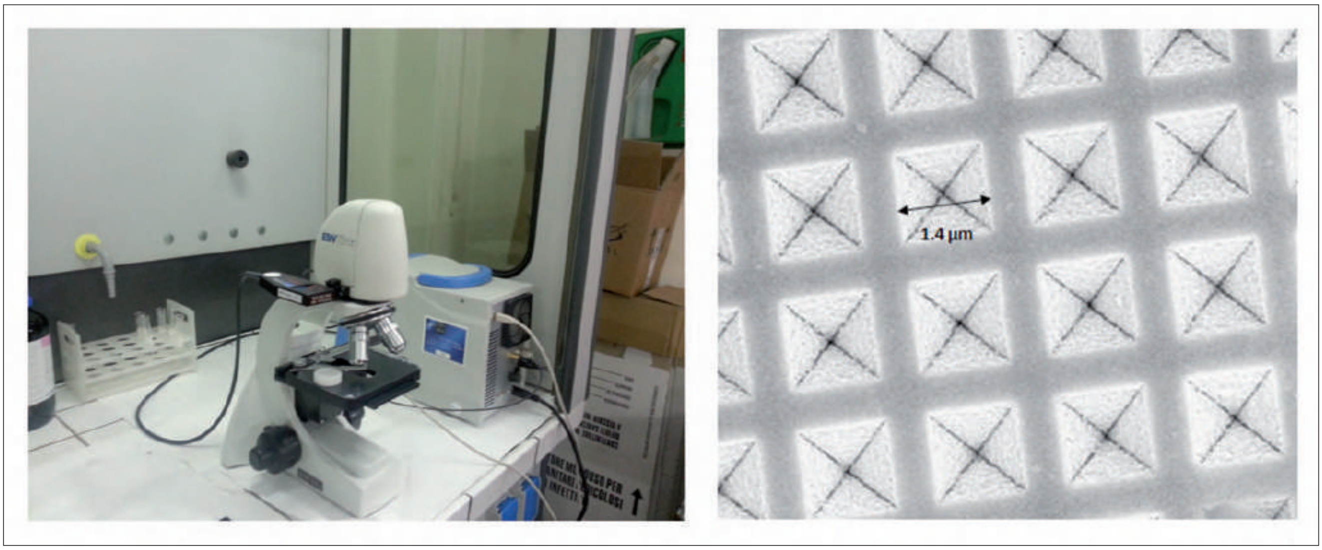


FIGURE 1 Micro Raman instrument (on the left) and SERS substrate (on the right) (image obtained with Scanning Electron Microscope (SEM) Leo1525, EHT=20 kW, WD=3 mm, aperture size=20 µm)

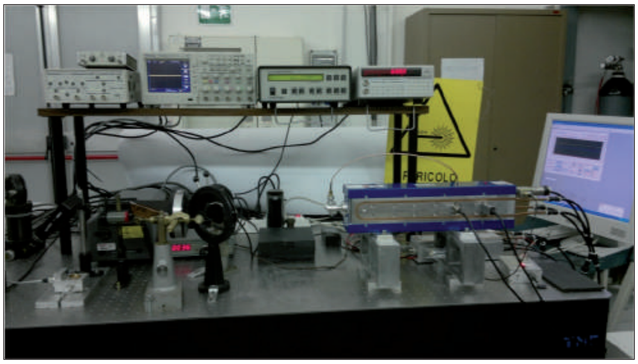


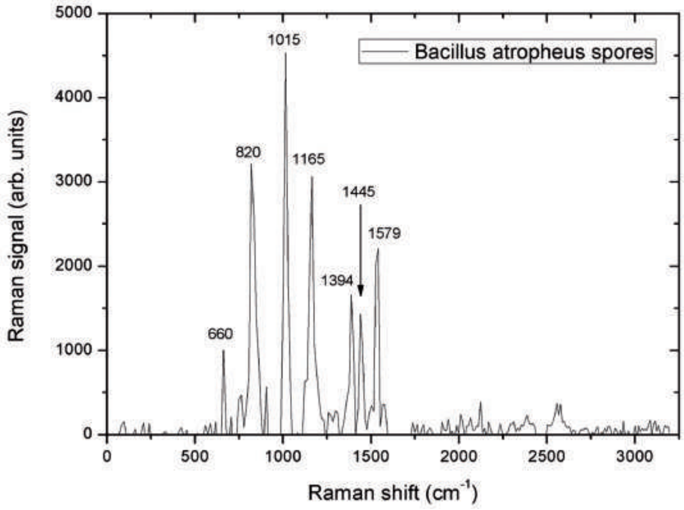
FIGURE 2 The LPAS apparatus with the control electronics in the background

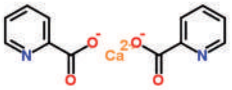
the Surface Enhanced Raman Spectroscopy technique (SERS technique), and in particular with i-Raman BWTek system (http://bwtek.com/technology/raman-systems/), characterized by laser source @785 nm, spectral resolution of 3 cm^{-1}, range from 0 to 4000 cm^{-1} and CCD array of 2048 pixel (Fig. 1, left). The spectra were obtained with an acquisition time of 10 s. The lenses utilized are: 4x, 10x, 20x, 40x, 80x, 100x. SERS substrate (Klarite®, Renishaw Diagnostics inc.) are composed of regular arrays of inverted pyramidal pits, realized by depositing an Au layer (Fig. 1, right) with an active area of 4 mm x 4 mm.

In order to increase the selective capture of the bacteria vegetative cells, the appropriate bacteriophages were immobilized on an active SERS substrate (functionalization). The bacteriophages are a type of viruses that by means of their receptors, which are highly selective and reactive towards specific bacteria, infect them. The functionalization of commercially available SERS substrates has been successfully accomplished with a fairly good and reliable fill factor.

Given that *B. anthracis* is classified as *Risk Group 3 (very high dangerous microorganism)*, *Bacillus thuringiensis* (ATCC 10792) and *Bacillus atrophaeus* var. *globigii* (ATCC 9372) were used as a simulant. This bacteria are generally used as models due to their phylogenetical similarity with the most hazardous species [11]. Cell and spore concentrations were carefully adjusted in the range between 10^6 and 10^4 CFU/ml, respectively, while 10 μl of solution was dropped on the SERS sensor active area.

The LPAS set-up adopts a compact (40x11x7 cm) CW CO_2 laser source emitting in the mid IR 9 – 10 μm wavelength range, operated without water cooling and frequency stabilized by a dedicated software inserted in a feedback loop. The laser is grating





Molecular vibration	Raman shift (cm^{-1})
Pyridine ring vibration (1)	≈ 660
C-COO$^-$ stretching	≈ 820
Pyridine ring vibration (2)	≈ 1015
Symm – COO$^-$ stretching	≈ 1394
Pyridine ring vibration (3)	≈ 1445
Asymm – COO$^-$ stretching	≈ 1579

FIGURE 3 SERS spectrum of *Bacillus atrophaeus* spores and band assignments

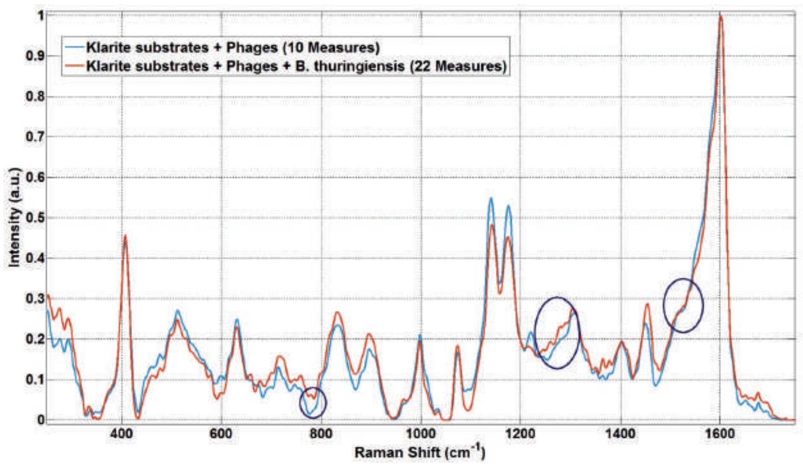


FIGURE 4 SERS spectra of vegetative cells of Bacillus thuringiensis (BT) on functionalized Klarite substrate

tunable through a single screw micrometer connected to a precise stepping motor, aimed at obtaining a computerized remote control (Fig. 2).

The LPAS apparatus has been implemented in discovering the possible methanol and melamine (2,4,6-triamino-1,3,5-triazine) contamination of food. The detection protocol is characterized by the absence of any requirement for chemical reagent purchase/disposal or sample pre-treatment and ease-of-use after initial method development. Spectra of methanol and ethanol alcohols were performed by the LPAS facility, arranged for the analysis of aqueous alcoholic mixtures directly in the photo-acoustic (PA) cell. Mixtures were analyzed at low alcohol concentration, down to 10 ppmv in water.

For monitoring milk adulteration with melamine, a home-made PA cell designed for analysis of solid mixtures was introduced in the LPAS apparatus.

Results

The detection of bacteria and spores, eventually dispersed in aerosol as biological weapons, can be obtained with a Raman spectrum of *B. atrophaeus* spores and *B. thuringiensis* vegetative cells (Fig. 3 and Fig. 4, respectively). The major constituent of the endospores is the dipicolinic acid (2,6-pyridinedicarboxylic acid; CaDPA) [5] is essential to the heat resistance, that for B anthracis spores represents 10 to 15% weight [12, 13]. A range of spectral features has been observed (660, 820, 1015, 1165, 1394, 1445 and 1549 cm^{-1}) mainly due to CaDPA, according to literature [13, 14] (Fig. 3, right).

The SERS spectra obtained to the Klarite® substrate functionalized with phages and inoculated with B. thuringiensis compared with Klarite® substrate functionalized without *B. thuringiensis* are showed in Figure 4.

Even if the spectra are very similar and, except for intensity, the phages signal is very strong and overlays that of the bacteria, slight differences are emerging around 1500 (very weak) 1300 and 800 cm^{-1} (Fig. 4, circle).

In order to highlight the spatial organization (e.g, a possible overlap between the attached molecules) of spores and cells, SEM investigation was performed on the same target material.

Figure 5 shows the SEM (LEO Gemini 1525 FEGSEM) images of spores of *B. atrophaeus* after deposition on the SERS sensor, while in Figure 6 the chain of vegetative cells for B. thuringiensis dispersed in physiological solution is shown.

The left image in Figure 5 highlights the organization of spores in clusters of some tenths or more on the SERS sensor, even if some individual, scattered spores are also visible (Fig. 5, right). That condition is the best to carry out measurements.

The vegetative cells of *B. thuringiensis*, suspended in a physiological solution and organized in chain, are showed in Figure 6. The images a) and b) were acquired with Optical Microscope (NIKON Eclipse E400) at magnification 100x, while the images in c) and d) were obtained with LEO Gemini 1525 FEGSEM. The dimensions of the cells are compatible with B. thuringiensis size and shape. The arrow indicates a possible endospore formation.

In the case of contaminants, additives or adulterants in goods and food, LPAS spectra have been performed in the framework of the SAL@CQO project, for pure ethanol and methanol, and presented in Figure 7, respectively. Comparing the two spectral profiles, significant wavelength-dependent differences are observable in terms of relative absorption intensity, as expected.

Several spectral studies were performed for ethanol/methanol mixtures in water as well, by mixing different relative amounts of the two alcohols [15]. The differences existing among the recorded spectra are stressed by the Principal Component Analysis (PCA) method operated on the experimental records and shown in Figure 8, as a 2D view. From this analysis, it comes out that the aqueous solutions of pure or diluted alcohols cover non-overlapping areas on the first two Principal Components chart. This result is promising, and a second step experimentation is planned to take into account the role of interfering substances and to construct calibration curves. In particular, the calibration will be based on the LPAS analysis applied to a set of alcoholic mixtures, selected to cover a concentration range finalized to a practical use. In a further step, experiments will be performed to validate the method. In the last step, finalized to the exploitation of the results, this proof of concept will be applied to the real-time detection of methanol level in commercial beverage products.

Food adulterants, such as melamine powder, were monitored by LPAS, being a material commonly used as a fertilizer and in the production of laminates, plastics, and glues. In recent years, a fraudulent adulteration with melamine has been reported in milk products and pet food. In 2007, adulteration of pet food by melamine determined the illness and death of the animals that consumed the contaminated product [16, 17]. Two years later, 300,000 cases of

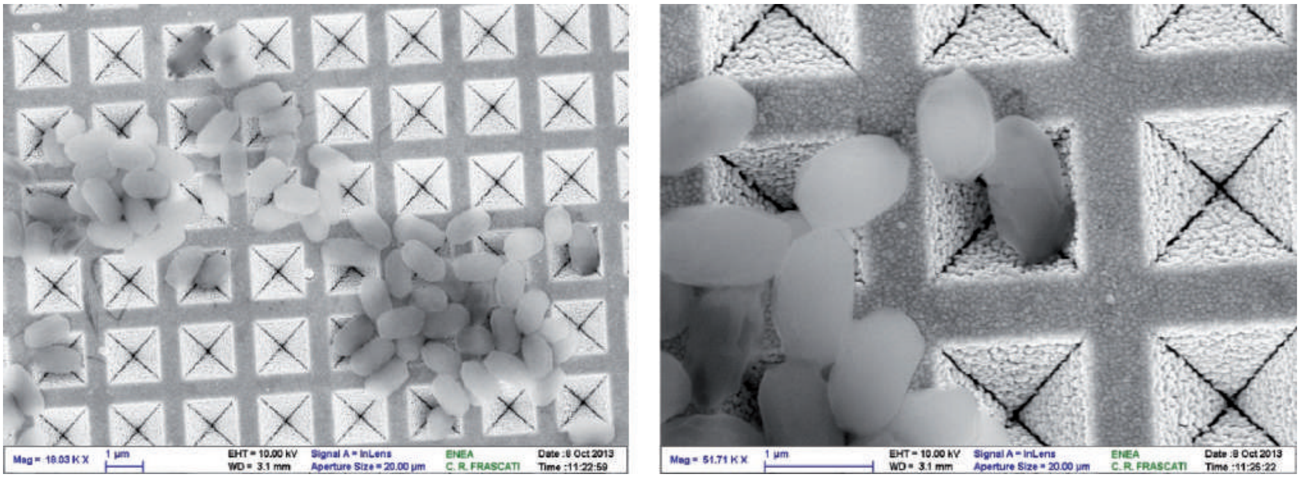


FIGURE 5 *Bacillus atrophaeus* spores SEM image (EHT=10 kW, WD=3.1 mm, aperture size=20 µm)

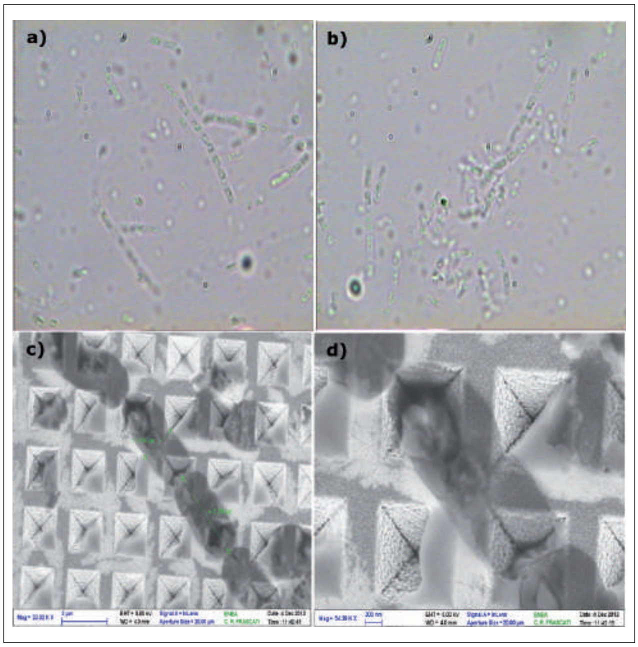


FIGURE 6 *Bacillus thuringiensis* cells organized in chain: a) and b): Optical Microscope images (NIKON Eclipse E400, magnification 100x); c) and d): SEM images LEO Gemini 1525 FEGSEM, EHT=5 kW, WD=4 mm, aperture size=20 μm

renal complications in children and at least 6 child deaths were ascertained in China, directly caused by milk adulterated with melamine. A reason for the adulteration of a food product with melamine is that its high nitrogen content increases the apparent protein content measured by standard analysis tests. This adulteration is difficult to reveal since standard chemical tests measure the total nitrogen content as an indication of the protein levels. The U.S. Food and Drug Administration (FDA) stated that a level of 1 ppm was a safe threshold for melamine in milk infant formula.

The LPAS spectra of pure milk and melamine mixtures are quite similar, but differences can be quantified in the statistical analysis presented in Figure 9. In this multivariate analysis it is evident that milk and melamine, as well as their mixtures, are clearly distinguishable from each other.

Conclusions

The easy-to-use sensors developed for early detection of biohazard in food and aerosols in the framework

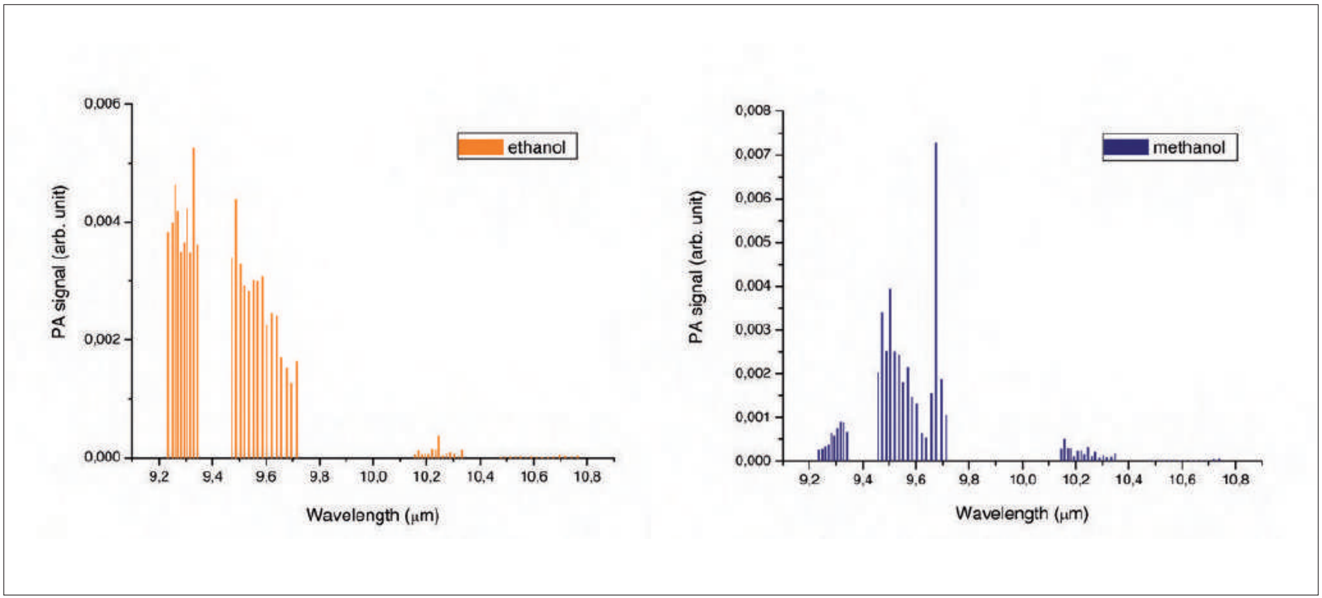


FIGURE 7 Photo-acoustic spectra measured with LPAS apparatus in the mid IR 9 – 10 μm wavelength range: pure ethanol (left); pure methanol (right)

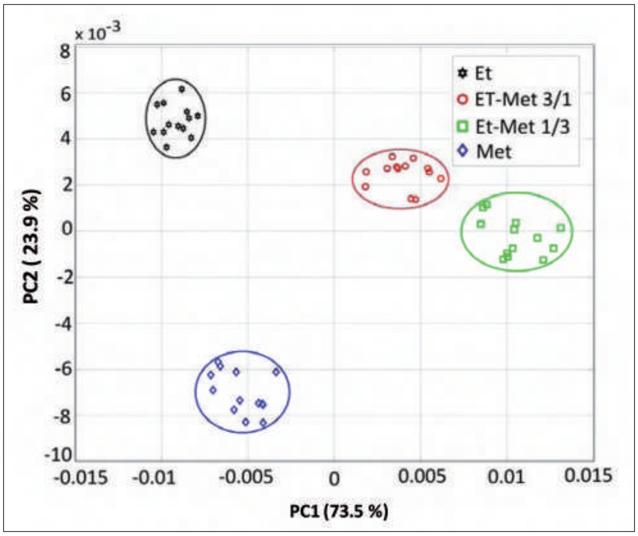


FIGURE 8 2D view of the PCA operated on ethanol/methanol mixtures in water, at different relative concentrations

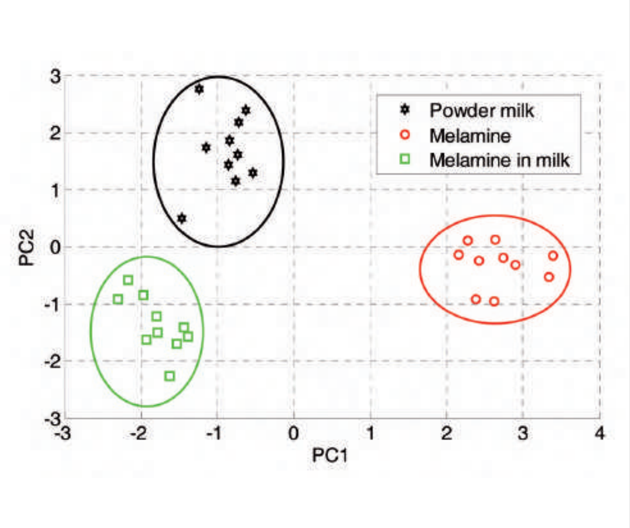


FIGURE 9 PCA result of the melamine experiment

of RAMBO and SAL@CQO projects have reached the capability for high-selectivity and sensitivity monitoring of both bacteria and contaminants.

In the case of bioterrorism attacks, SERS measurements were successfully performed even on few spores and cells, demonstrating its high sensitivity for early warning of biological threats. As for spores, the SERS spectra exhibited a satisfactory S/N ratio to identify the main spectral features that have been assigned to CaDPA. Also for cells originated from vegetation (like pollens), the spectra were assigned, even if the breakable physiology of the bacteria makes experiments more complicated. Work is in progress to define a routine data processing, that will allow to recognize and classify each spectrum on the basis of its peculiar SERS peaks.

The SAL@CQO project is aimed at developing and applying innovative, easy-to-use product-instruments to be used in production chains for performing a quality screening prior to food commercialization. The continuous monitoring of quality and preservation of food has been demonstrated by LPAS in distinguishing the presence of a specific additive in the relative food matrix by means of a multivariate analysis. The validation of the method is in progress, in cooperation with the Italian National Institute of Health (ISS) for a specific case study. The final demonstration will be based on the detection of a single food adulteration.

Acknowledgements

The authors give special thanks to Dr. Alessandro Rufoloni, Technical Unit for Nuclear Fusion - Superconductivity Section, for providing the SEM images.

Antonia Lai, Salvatore Almaviva, Valeria Spizzichino,
Lorella Addari, Gianfranco Giubileo, Giovanni Dipoppa, Antonio Palucci
ENEA, Technical Unit for the Development of Applications of Radiation -
Diagnostics and Laser Metrology Laboratory

references & notes

[1] G. Christopher, T.J. Cieslak, J. Pavlin, E. Eitzen, 1997, “Biological Warfare; a historical perspective”, in JAMA, 278(5), 412-417.

[2] F. Frischknecht, 2003, “The history of biological warfare. Human experimentation,modern nightmares and lone madmen in the twentieth century”, in EMBO reports 4 (special issue).

[3] Inglesby et al, 1999, “Anthrax as a biological weapon. Medical and public health management”, in JAMA, 281,1735-1745.

[4] P. Stagier, R. Losick, 1996, “Molecular genetics of sporulation in Bacillus subtilis”, in Annu. Rev. Genet., 30, 297-341.

[5] P. Setlow, 2006, “Spores of Bacillus subtilis: their resistance to and killing by radiation, heat and chemicals”, in J. Appl. Microbiol. , 101, 514–525.

[6] W.L. Nicholson, P. Setlow, 1990, “Sporulation, germination and outgrowth”, in C.R. Harwood, S.M. Cutting, (Eds) Molecular Biological Methods for Bacillus, Wiley, West Sussex, 391-450.

[7] S.J. Foster, K. Johnstone, 1990, “Pulling the trigger: the mechanism of bacterial spore germination”, in Molecular Microbiology, 4(1), 137-141.

[8] N.A. Logan, 2004, Safety of aerobic endospores forming bacteria. In: Ricca E., Henriques AO., Cutting SM, (Eds) Bacterial Spores Formers-Probiotics and emerging Applications Horizon Bioscience, Norfolk, 93-106.

[9] J.A. Jerningan et al, 2001, “Bioterrorism-related inhalational anthrax: the first 10 cases reported in the United States”, in Emerg. Infect. Dis., 7, 933-944.

[10] Requirements of European Union to meet quality standards are described in: Commission Directive 89/362EEC Document 389L0362; Council Directive 92/46/EEC Document 392L0046; Commission Decision 396/036 Document 396D0360.

[11] C. Ash, J.A.E. Farrow, S. Wallbanks, M.D. Collins, 1991, “Phylogenetic heterogeneity of the genus Bacillus revealed by comparative analysis of small subunit-ribosomal RNA sequences”, in Lett. Appl. Microbiolo., 13, 202-206.

[12] F.W. Jansen, A.J. Lund, L.E. Anderson, 1958, “Colorimetric assay for dipicolinic acid in bacterial spores”, in Science, 127, 26-27.

[13] H. Liu, N.H. Bergman, B. Thomason et al, 2004, “Formation and composition of the Bacillus anthracis endospores”, in J. Bacteriology, 186, 164.

[14] S. Stockel, W. Schumacher, S. Meisel, M. Elschner, P. Rosch, J. Popp, 2010, “Raman Spectroscopy-Compatible Inactivation Method for Pathogenic Endospores”, in Applied and Environmental Microbiology, 76, n. 9, 2895-2907.

[15] J.W. Lin, S.Y. Shaw, 2009, “The potential of CO$_2$ laser photoacoustic spectrometry for detection of methanol in alcoholic beverage”, in Appl Phys B, 94, 535–544.

[16] J.R. Ingelfinger, 2008, “Melamine and the Global Implications of Food Contamination”, in New Engl. Jnl. Med., 359, 2745.

[17] L.J. Mauer, A.A. Chernyshova, A. Hiatt, A. Deering, R. Davis, 2009, “Melamine Detection in Infant Formula Powder Using Near- and Mid-Infrared Spectroscopy”, in J. Agric. Food Chem., 57, 3974–3980.

Sistema di supporto alle decisioni finalizzato al miglioramento della “protezione fisica” di infrastrutture critiche in caso di calamità naturali

La fornitura dei servizi essenziali dipende dall’integrità ed efficienza di numerose reti tecnologiche “critiche”, quali, ad esempio, le reti elettriche, le reti di telecomunicazioni, acquedotti e gasdotti, reti viarie e ferroviarie. È responsabilità di ciascuna nazione proteggerle con cura e, in collaborazione con gli operatori pubblici e privati che le possiedono e le controllano, realizzare gli strumenti appropriati per aumentarne la resilienza in situazioni di crisi, indotte da eventi meteo avversi, da catastrofi naturali. Quest’articolo descrive i lavori attualmente in corso nell’ambito di progetti nazionali ed europei per la realizzazione di un Sistema di Supporto alle Decisioni (DSS, Decision Support System) in grado di analizzare e prevedere costantemente il livello di rischio al quale sono sottoposte le infrastrutture, valutando in anticipo gli impatti e le conseguenze della loro perdita di funzionalità. Questo consentirà a operatori pubblici e privati di prevenire situazioni avverse e approntare le opportune misure di emergenza e di mitigazione per ridurre o evitare le conseguenze di un pericoloso blackout dei servizi.

Decision Support System aimed at improving the “physical protection” of critical infrastructures against natural events

Nowadays, the delivery of essential services depend on the integrity and efficiency of a set of critical technological networks as for example, electrical grids, telecommunication networks, gas and water pipelines, roads and railways. It is the responsibility of each nation to protect them carefully and, in collaboration with the operators (public and private) that own and control them, realize appropriate tools to increase their resilience against crisis scenarios which might be opened by adverse natural hazards and seismic events. This work describes the ongoing work within the framework of national and European projects for the construction of an operating Decision Support System (DSS) able to continuously evaluate and predict the level of risk to which infrastructures are subjected, by assessing in advance the impacts and consequences of their loss. This allows public and private operators to prepare themselves and set up appropriate emergency and mitigation plans to reduce or remove the consequences of a dangerous blackout of services.

DOI: 10.12910/EAI2014-92

■ *A. Di Pietro, L. La Porta, M. Pollino, V. Rosato, A. Tofani*

■ **Contact person: Vittorio Rosato**
vittorio.rosato@enea.it

Introduction

Critical Infrastructures (CI) are technological systems (e.g., gas and water pipelines, telecommunication networks, electrical grids, roads and railways) the correct functioning of which impacts on the life quality of citizens. CI protection is needed to guarantee their physical integrity and the continuity of the services they deliver. Critical Infrastructure Protection (CIP) is thus a major issue of nations, also due to its trans-national relevance. EU has thus issued directives to Member States (MS) in favor of an increased level of protection, thus recognizing the fact that they constitute a unique, large system covering all the EU area (EU Directive, 2008/114/CE).

Resilience (i.e., the ability of a system to recover its equilibrium state after a perturbation) is thus becoming a keyword in this domain. Wherever vulnerability could be decreased down to a certain extent - risks related to the occurrence of common cause failures could be appropriately mitigated, as well as those resulting from human causes - there are natural threats resulting from adverse meteorological and geo-physical events which can be hardly mitigated although they could be, in many cases, at least reliably predicted. The focus has thus been diverted from vulnerability to resilience. The goal will be thus reducing the systems' vulnerability and increasing their resilience.

This task has been attempted, at a federal level, in the U.S. by the creation of a National Infrastructures Simulation and Analysis Centre (NISAC) [1], which plays the role of connecting all national-wide CI operators and systems in a unique site able to analysing and forecasting high-impact natural hazards and the consequent faults on CI and the environment. This should, in principle, favour risk prediction (mainly due to natural hazards) and the set-up of appropriate mitigation and healing strategies in advance. This has been proven to produce some enhancement of the systems' resilience, a better control of dependency phenomena (i.e., those related to the physical and functional dependencies between one infrastructure and the others) and, thus, to prevent cascading effects. Much in the same spirit, the EU-funded Network of Excellence CIPRNet (Critical Infrastructures Preparedness and Resilience Research Network) [2] aims at proposing the NISAC experience in Europe by sustaining the technological and institutional growth of European Infrastructures Simulation and Analysis Centres (EISAC), a constellation of connected national centres enabling a 24/7 risk analysis of the CI elements, providing these data to the appropriate national authorities appointed for CIP. The realization of EISAC national nodes has been demanded to local partners of the CIPRNet network. To this aim, ENEA has inserted the realization of the first seed of the Italian EISAC node into the project "RoMA" (Resilience enhancement of a Metropolitan Area), which has been recently approved and funded by MIUR (the Italian Ministry of Research) in the frame of the Call "Smart Cities and Communities".

From the technical side, the CIPRNet project aims at designing and developing a number of technological tools which will boost the EISAC nodes, by allowing them to operationally sustaining the task of assessing the state of risks of the CI. Among others, there is a Decision Support System (DSS hereafter), the structure and design of which will be the object of the present report.

A major role in the construction of such a tool is played by the GIS (Geographical Information Systems) technologies. In the last few years, the geo-scientific community has been focusing on the use of GIS technologies and techniques for supporting natural disaster early warning and emergency management tasks [3]. The need for related standards and effective spatial DSS, based on a GUI (Graphical User Interface) with geo-visual analytic tools, has been recognized by numerous researchers, as shown by several on-going research activities. Multi-source data and GIS-integrated analysis can contribute to a better emergency planning, providing fundamental information for immediate response [4].

Risk assessment of CI

At the bases of a DSS loop, there is the need of estimating a number of factors which determine the "risk" that the occurrence of a given event might cause in the technological systems. Then, at the end of a thorough estimate of the risk, the system is also called to provide operators and emergency managers with insights usable for supporting decision-making. The DSS workflow shown in this report fulfils just the first task, i.e., estimating the risk and presenting the more complete and consequence-based risk evaluation. The technological activities of the CIPRNet project also encompass the creation of a "What-if" support tool, enabling operators to estimate the impacts that possible mitigation and healing procedures might produce in the critical scenario, thus completing the set of tools supporting operators.

Let us thus define $R(T_i, CI_j^x)$the Risk associated with the loss (or the functionality reduction) of the element CI_j^x (x-th element of the j-th infrastructure) due to a natural threat T_i

$$R(T_i, CI_j^x) = Pr(T_i)\ V(CI_j^x, T_i) I(CI_j^x) \qquad (1)$$

where:

- $Pr(T_i)$ is the probability of occurrence of the threat T_i
- $V(CI_j^x, T_i)$ is the vulnerability, w.r.t the threat T_i, of the x-th element of the j-th infrastructure
- $I(CI_j^x)$ is the sum of impacts and consequences that the absence of the x-th element of j-th CI produces upon failure:
  - in its network and in the other CI networks functionally related to it;
  - on the environment and the population affected by the failure.

The Risk equation (1)

- depends on the composition of 3 factors, which determine the value of the Risk.
- makes reference to a specific threat *manifestation*. A natural hazard (say a tropical typhoon) constitutes a threat for the CI systems as it is associated to several "physical manifestations" (like, e.g., abundant rainfalls, strong wind, lightening, etc.) which may impact on the infrastructures producing harm (i.e., winds could highly stress mechanical structures, flooding could strike on physical CI elements located in flooded areas, lightning could damage electrical systems, etc.). In this respect, we will use T_i to indicate a specific *manifestation* of a given natural hazard; for a given predicted natural hazard, we will specify which of its manifestations will be used to evaluate the Risk of eq.(1).

Impacts indicate the reduction (or loss) of services. They will thus be estimated by using the metrics of Quality of Service (QoS): upon specific physical damage produced by threat manifestations on CI elements, the struck CI and the other ones (where services depend on that delivered by the injured one), will presumably reduce (or even completely lose) their QoS with respect to their standard operating levels. Impacts, moreover, could be "weighted" in terms of the consequences they will produce on:

1. population (in terms of people affected by outages, to be "profiled" in terms of vulnerability area which they belong to)
2. primary services (reduction of functionality in hospitals, schools, public transportations, etc.)
3. the environment (if the impacts are associated to environmental damages, such as pollution, land contamination, etc.)
4. industrial sectors (in terms of reduction of productivity, loss of GDP, etc.)

Eventually, the estimate of Risk through eq.(1) will provide CI operators, emergency responders, public authorities with a comprehensive assessment of the amplitude of the crisis they will be presumably going to face. The awareness of these data will allow a knowledge-based set-up of mitigation and healing plans.

DSS workflow and function

The DSS designed in the CIPRNet project to evaluate the state of Risk of the CI elements in a given area will make a thorough evaluation of eq. (1) by using existing and ad-hoc developed technological tools (databases, simulation models), integrated with existing technologies (now-casting and remote sensing, with High Resolution and SAR data). The DSS can leverage on proprietary Databases and external repositories, containing different typologies of data: Territorial and Environmental, Socio-economical (e.g., Census data), Technological Infrastructures data, Natural hazards/events (e.g., earthquakes catalogue, landslides, flood risk, etc.).

Figure 1 reports a schematic layout of the different tasks that the designed workflow should accomplish in order to produce a "CI Risk Daily Report", which will

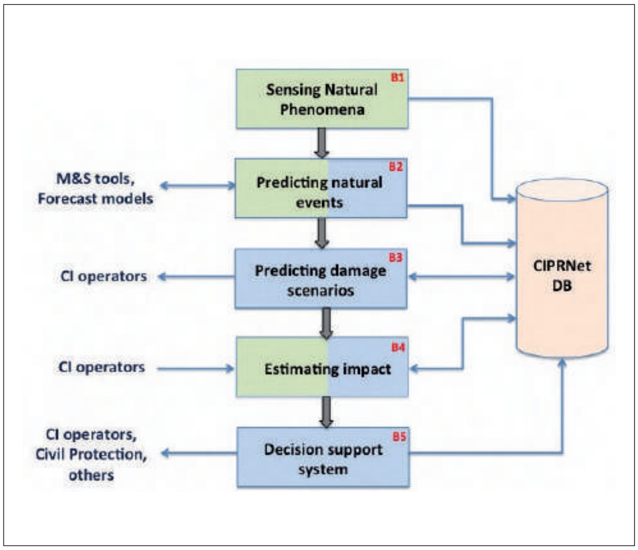


FIGURE 1 DSS Workflow. Different colours shading action boxes indicate technologies directly produced in the CIPRNet project (blue) and data/technologies taken from third parties or externally provided data (green)

constitute the specific outcome of the EISAC nodes in favour of their main end users: Civil Protection Depts. and/or other Public Authorities committed to CIP.

In the following, we will describe the DSS workflow, which is composed of five action boxes (see Fig. 1). Each of them contributes to evaluate the Risk as expressed in eq.(1). It is worth stressing that this is a workflow in collaboration with CI operators, who will be called to comply with and contribute to the risk assessment, as shown in the following.

In the first action (the first term on the right-hand side of eq. (1)), the system collects information from the field (through proximal or remote sensors) and from weather forecast (medium-long term as weather forecast, and short-term by now-casting systems [5]). High resolution downscaling of weather forecast will be performed in areas where a higher forecast resolution would be significant for increasing prediction reliability (e.g., Fig. 2 and Fig. 3). According to these data it is possible to make estimated maps

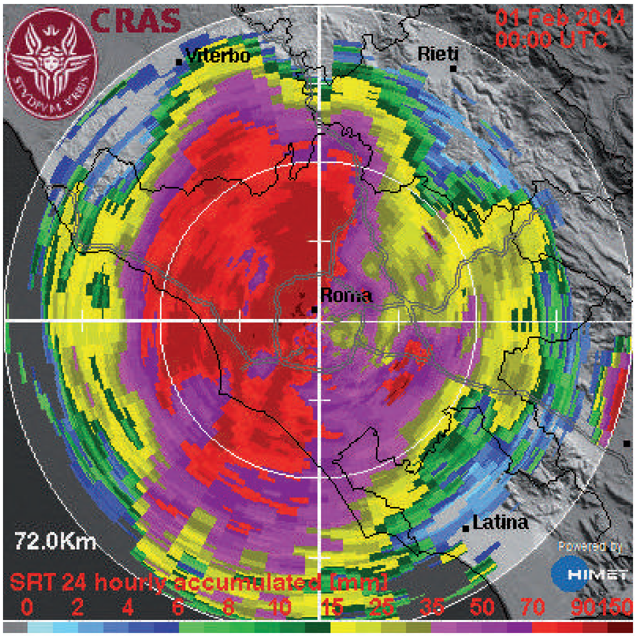


FIGURE 2 The cumulate 24h prediction from a now-casting radar showing the rain abundance on the city of Rome (data taken on January 31, 2014, when a strong precipitation hit the city of Rome). Courtesy of Himet Srl

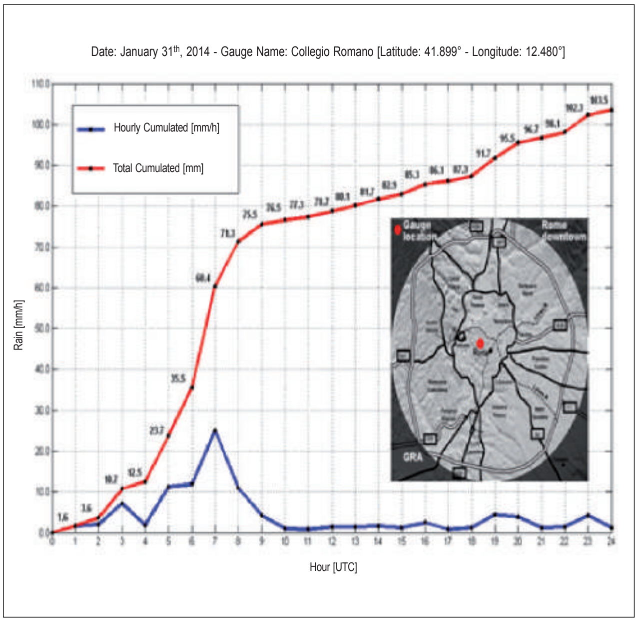


FIGURE 3 The hourly and the cumulated amount of rainfall in Rome on January 31, 2014. The red spot represents the location of the now-casting radar. The red line is the cumulated rainfall, the blue one is the hourly value. Data in mm/hour. Courtesy of Himet Srl

of hourly precipitations, which could then be used to assess the potential impact on CI.

In the second action (the second term on the right hand side of eq. (1)), starting from the event prediction, the system analyses its database to establish the probability that a given infrastructural element is hit by the threat and damaged. Intrinsic vulnerabilities of elements are correlated with the event probability and with its predicted strength in order to provide a damage probability. This information will be integrated, in the third action, into a "Harm Scenario" (i.e., the set of all CI elements possibly hit by one or more of the predicted threats). In this framework, one of the main aims of the DSS is to make geographic data, thematic maps and probable "Damage Scenarios" available to specific end users (and, potentially, to the public). To this end, the system allows end users to view spatial data (Fig. 4) within a suitable web-interface, by means of a WebGIS application (e.g., a customizable and totally user-specific geospatial platform). Such a tool provides interactive query capabilities and integrates the GIS-based solutions with other technologies.

At this stage, the workflow envisages the communication of the expected Damage Scenarios to CI operators; these latter will be called to evaluate, with their own simulation tools, the impact (in terms of reduction of functionality) on their networks should the predicted outages of the elements reported in the Harm Scenario effectively occur. In turn, CI operators will reply by identifying the Impacts on their services that the different types of damage would produce - e.g., in terms of reduction of QoS in specific points of their networks.

The fourth action of the workflow will then start. The DSS system will gather the information from the CI operators and, by using specific tools accounting for the system's functional dependences (or interdependencies), will evaluate the overall impact of the predicted harm on

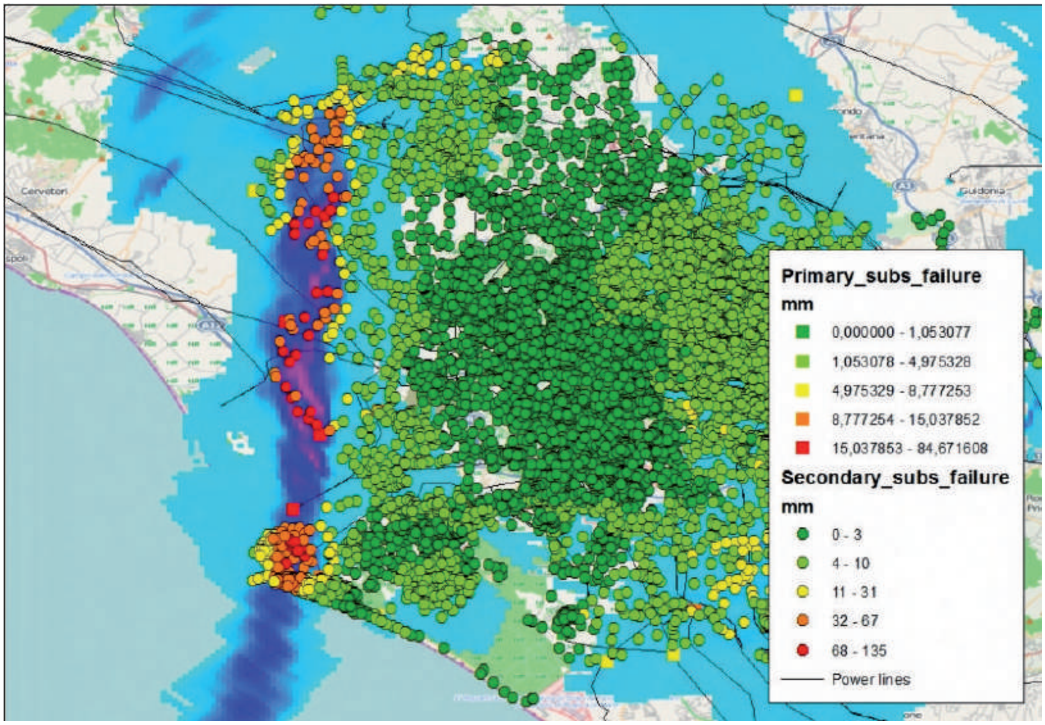


FIGURE 4 Damage scenario with the area of predicted over-threshold precipitations (blue shaded area) and the prediction of potentially affected CI elements (red dots)

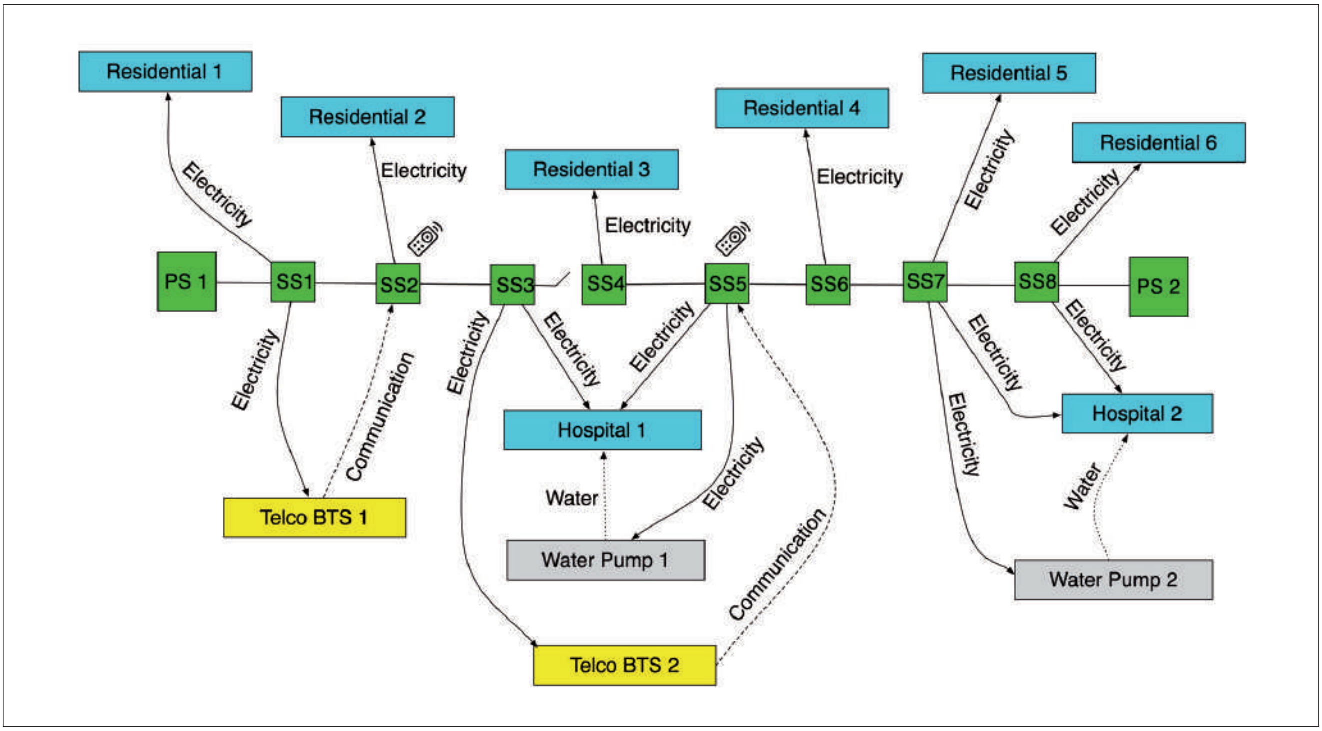


FIGURE 5 An example of an abstract interdependency model that represents the interactions existing among different systems providing services to one another. Green boxes represent electrical substations

the whole CI system (at a level of "system of systems"). In particular, this task will be performed by using appropriate modelling tools (e.g., I2SIM [6]) which, at specific granularity level for the description of the CI present in a given area, will contain their functional dependence useful for estimating the probability of possible cascading effects and feedback loops present among the CIs (Fig. 5). Negative feedback loops, in fact, could amplify and increase the impacts on the infrastructures and add to the overall effects of the outages.

In the fifth layer, the overall scenario description (in terms of functionality reduction or loss of one or more CI) will be "weighted" by estimating the consequences that those complete or partial outages in services might produce in the 4 sectors recalled above. This analysis is carried out by leveraging on "specific vulnerability" indices (i.e., the loss of "well-being" of a specific sector, estimated with some metrics, with respect to the loss of a unitary decrease in a given service, such as electricity, water, gas, telecommunications, etc.). This information will be useful to CI operators and emergency managers to perceive in depth the consequences of the crisis that they will be called to face.

Conclusions

Following the theoretical framework of eq. (1), the DSS workflow evaluates on a 24/7 basis the state of "Risk" of the CI elements in a given area, due to natural threats (as for example flooding, strong wind, heavy rain, heavy snow and hot wave). The various information achieved at the end of the DSS workflow, both quantitative (CI elements risk maps) and qualitative (daily reports concerning impacts and consequences of predicted natural extreme events on different sectors), represent a significant advancement with respect to the current capabilities: (a) the scenario is "predicted", thus it will be delivered to decision-makers prior to the event occurrence; (b) the workflow will also evaluate possible cascading effects due to the more or less evident system's dependencies, thus increasing the impact predictions based on single-infrastructure evaluations; (c) other than impacts at the physical and service levels, the DSS will correlate impacts data with different types of information layers (physical, environmental, territorial, industrial, economic, social), and will be able to establish further types of impacts: on the population, on the different industrial sectors, on the environment. Moreover, the webGIS advanced interface allows the DSS end users to visualize CI elements risk maps and overlay this information with other kinds of information as, for example, impact and consequence analysis results. In particular, on the environmental side, the system could also be used for predicting the course of events in the cases where the CI damage scenario would imply some event (such as oil spill, toxic or radioactive releases from plants, etc.). In such a case, the DSS could interact with specific simulation models (ocean dynamics, gas transport in the atmosphere, etc…) for the prediction of environmental impacts.

Acknowledgement

This work was developed from the FP7 Network of Excellence CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged. The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

Antonio Di Pietro, Vittorio Rosato, Alberto Tofani
ENEA, Technical Unit for Energy and Environmental Modeling
Computing and Technologic Infrastructures Laboratory

Luigi La Porta, Maurizio Pollino
ENEA, Technical Unit for Energy and Environmental Modeling
Earth Observations and Analyses Laboratory

references & notes

[1] NISAC: http://www.sandia.gov/nisac/
[2] CIPRNet EU FP7 project: www.ciprnet.eu
[3] M. Pollino, G. Fattoruso, L. La Porta, A.B. Della Rocca, V. James, 2012, "Collaborative Open Source Geospatial Tools and Maps Supporting the Response Planning to Disastrous Earthquake Events", in Future Internet, 4, 451-468.
[4] V. Rosato, A. Di Pietro, G. Aprea, R. Delfanti, L. La Porta, J.R. Marti, P. Lusina, M. Pollino, 2012, Interaction between environmental and technological systems: toward an unifying approach for Risk Prediction, CRITIS - 7th International Conference in Critical Information Infrastructures Security.
[5] Now-casting systems consist in X-, or C-band radar. They are mostly pulse-Doppler radars capable of detecting the motion of rain droplets in addition to the intensity of the precipitation. Both types of data can be analyzed to determine the structure of storms and their potential to cause severe weather conditions. They usually span a range of 100 Km of radius, thus providing a direct assessment of the raindrops in the clouds, the estimate of their abundance, and the velocity of the storm front.
[6] J.R. Marti, J.A. Hollman, C. Ventura, and J. Jatskevich, 2008, "Dynamic recovery of critical infrastructures: real-time temporal coordination", in International Journal of Critical Infrastructures, 4, no. 1, 17–31.

Qualità di servizio di una rete elettrica sotto attacchi informatici al suo sistema di controllo, supervisione e acquisizione dati

L'articolo descrive modelli per rappresentare un sistema di Controllo, Supervisione e Acquisizione dati (SCADA, Supervisory Control And Data Acquisition) di una rete elettrica e la sua rete aziendale sotto diversi attacchi informatici: malware propagation, Denial of Service (DoS) e Man In The Middle (MITM). Abbiamo utilizzato NetLogo per identificare la propagazione del malware, in relazione alle politiche di sicurezza per il sistema SCADA e la rete aziendale, adottate dall'operatore della rete elettrica. Inoltre, le conseguenze di tali attacchi sulla Qualità del servizio (QoS) del sistema SCADA e della rete elettrica sono state calcolate mediante il simulatore di rete NS2.

Quality of Service of an electrical grid under cyber attacks to its supervisory control and data acquisition system

This paper describes models to represent a Supervisory Control And Data Acquisition (SCADA) system of an electrical grid and its corporate network, under malware propagation, Denial of Service (DoS) and Man In The Middle (MITM) attacks. We use NetLogo to identify possible malware propagation in relation to SCADA & corporate security policies adopted by the electrical utility. The consequences of such attacks on SCADA's Quality of Service (QoS) and, in turn, on the QoS of the electrical grid have been computed by NS2 network simulator.

DOI: 10.12910/EAI2014-93

■ *E. Ciancamerla, B. Fresilli, M. Minichino, S. Palmieri, T. Patriarca*

Introduction

SCADA encompasses systems that monitor and control the industrial infrastructure, such as electrical grids. Since SCADA systems directly control physical systems, availability and reliability come in the first place, whereas in ICT (Information and Communication Technology) networks a significant stress is laid on confidentiality of information. Born as isolated systems, SCADA's carry the burden of a legacy of trust in the network, thus they lack the tools for monitoring and self-protection that have long been integrated in ICT networks. For instance, their logging capabilities are geared towards disturbances rather than security attacks [1]. Contrary to ICT network devices, SCADA systems are designed to run for years on end [2] without any reboot. This complicates the application of software patches and even makes post-attack forensics problematic since the system cannot be taken down and analyzed at wish [1]. In this work, we consider an actual reference scenario identified within the MICIE EU project (http://www.micie.eu) first and then extended within the ongoing CockpitCI (http://www.cockpitci.eu) EU project. We represent SCADA and corporate network under malware propagation, Denial of

■ Contact person: Michele Minichino
michele.minichino@enea.it

Service and Man In The Middle attacks. We use NetLogo (http://ccl.northwestern.edu/netlogo/) to model and analyse malware propagation in relation to the adopted SCADA & corporate network security policies, and NS2 (http://www.isi.edu/nsnam/ns/) to compute the consequences of the attacks on SCADA performances and, in turn, on power grid functionalities.

Reference scenario

The reference scenario limits the extension of the real world to be included into the models and provides a concrete context of operation. It is composed by an actual SCADA, a 22 kV MV grid and a portion of the corporate network. Topologies, main functionalities, devices, links among devices, communication protocols - with special attention on TCP/IP based protocols [3] - interdependencies, cyber security issues, such as cyber threats, vulnerabilities, pre-existent cyber security policies & technical solutions and attack cases, are described within the reference scenario (http://www.cockpitci.eu). Figure 1 shows a simplified schema of the Medium Voltage (MV) electrical grid controlled by SCADA. It consists of a portion of a MV grid at 22 kV, energized by two HV/MV substations. Each substation feeds different types of loads/customers, throughout electrical sections, connected to one another by Normally Close Circuit breakers. The substations include Protection breakers. Under normal operative conditions, customers are energized by either one substation (TF) or the other one (CB), by means of two sub grids, separated from one another by two, Normally Open, Tie switches. Tie switches and Circuit breakers are remotely controlled by SCADA via its Remote Terminal Units (RTU). SCADA monitors the grid status, acts on Circuit breakers to connect or isolate the grid electrical sections, and on the Tie switches position to feed a subgrid by the alternate substation, in case of power grid reconfiguration on permanent electrical failure in the subgrid.

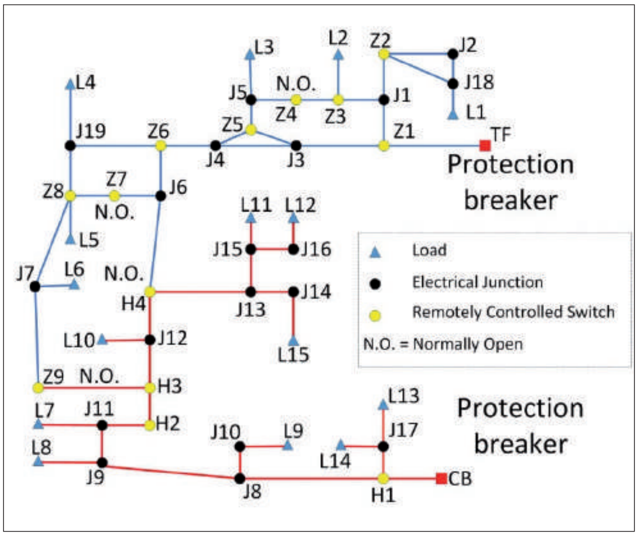


FIGURE 1 MV power grid

Figure 2 shows the SCADA system and a portion of corporate network of Israel Electric Corporation. From the SCADA Control Centre (SCC), the operator remotely controls in real-time the electrical grid in Figure 1, by means of RTUs. Particularly, the following devices belong to the SCADA system:

- MCPT G.W gateway, which converts a proprietary Data Link Communication (DLC) protocol for Radio channels to the TCP/IP protocol. For DLC and TCP/IP protocols, each transmission is automatically accompanied by an ACK message, ensuring the transmission integrity.
- Field Interface Unit (FIU MOSCAD), dedicated to RTU interrogation and routing of data messages to/from SCC. It comprises a Radio Frequency (RF) Modem Interface (RF Modem ND), that includes two VHF radio units (F2, F3) connecting the RTUs to SCC throughout either the F2 or F3 channel.
- Store & Forward (S&F) Repeater MOSCAD DN, which communicates upwards with the SCC (via the RF Modem and FIU) and downwards with the RTUs using the two RF channels (F1 and F3).
- RTUs; there are 13 RTU sites, 9 of them fed by TF substation and 4 by CB substation (Fig. 1).

The SCADA system is fully redundant. The main communication path between SCC and the RTUs traverses the main Gateway (MCPT G.W PRIME) and the main FIU (MOSCAD ND). In case of failure on the main path, data are rerouted on the backup path that traverses the backup Gateway (MCPT G.W SECOND), the backup FIU (MOSCAD DN), the corporate network from Point of Presence (PoP) ND to Local eXchange DN-VHF), MOSCAD DN S&F Repeater and then reaches the RTUs.

In case the primary RF channel is not available for any reason, the system switches to the alternate RF channel.

The portion of corporate network in the reference scenario is also shown in Figure 2. It is composed by three hierarchical layers:

- *A Backbone layer,* where PoP devices are connected to each other in a meshed topology (NA, NM and ND devices in Fig. 2). The PoP is a multiservice optical platform that integrates several technologies, including Synchronous Digital Hierarchy, Synchronous Optical Network (SDH/SONET) and Dense Wavelength Division Multiplexing (DWDM),
- A *Local eXchange layer* (LeX) represents the point of access at lower bandwidth of corporate network. In Figure 2, the following LeX devices: CB, ML, TF, MS, BL, DN-VHF.
- *A Transit eXchange layer* (TeX), between the two other layers, that grants scalable traffic in multi-ring topology. A TeX device is based on the SDH/SONET technology, which aggregates data flows at different bit rates and retransmits them over long distances.

Within the reference scenario, the SCADA operator executes a procedure, named FISR (Fault Isolation and System Restoration), to locate, isolate and quickly and safely reconfigure the electrical grid on permanent electrical failures. Permanent failures may cause the de-energisation even of a large part of electricity customers. We discuss how cyber threats, vulnerabilities and attacks might result in loss of view and loss of control of the electrical grid from the SCADA Control Centre and then, as a consequence, in a de-energisation of grid customers.

Scada cyber security

Cyber vulnerabilities and attack vectors of SCADA challenge the reliability, resiliency and safety of the electric grid day by day. For such a reason, a cyber security protection of SCADA & corporate network cannot be neglected by electrical grid utilities. Vulnerabilities involve computer, communications (SCADA & corporate

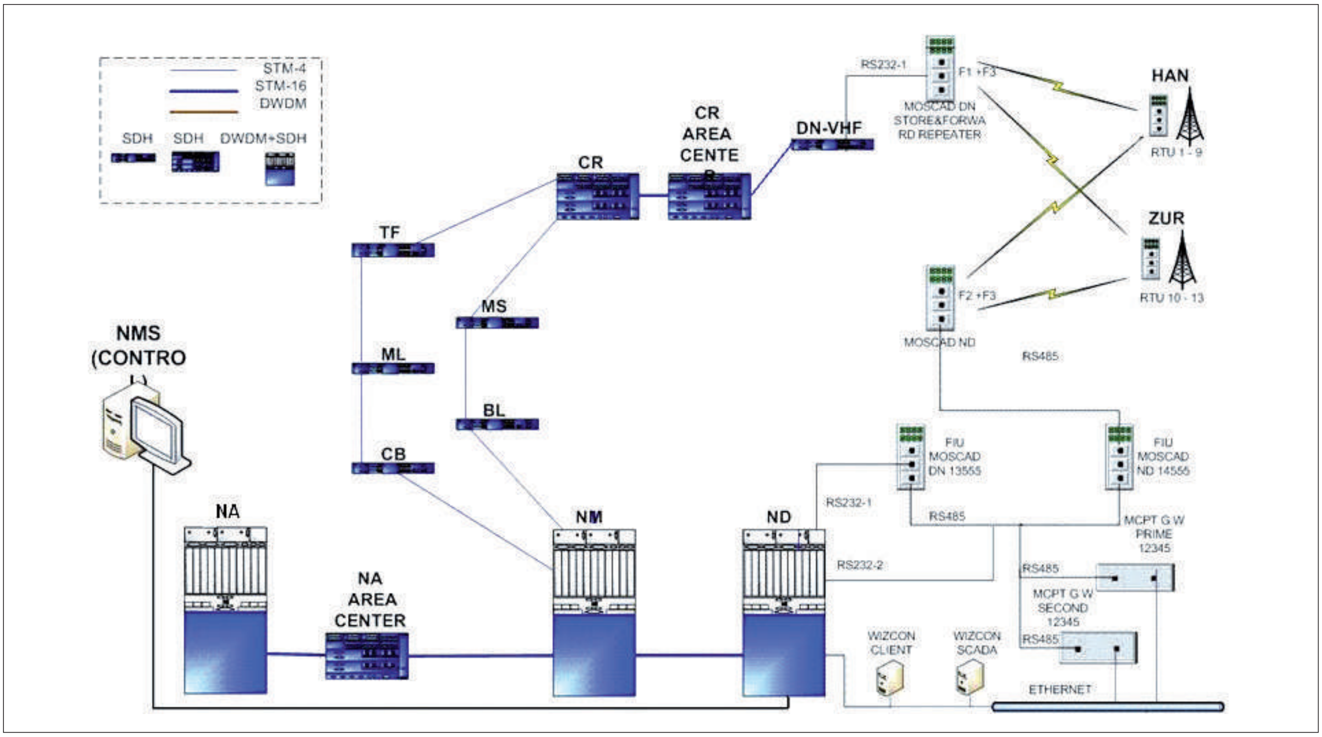


FIGURE 2 The SCADA system and a portion of corporate network

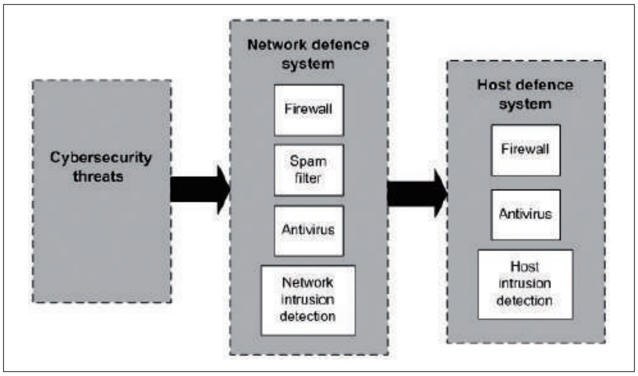


FIGURE 3 A typical cyber security protection system
Source: CockpitCI EU project

networks) and in turn electrical grids. Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously, and can come from many places, including indirectly through corporate network. As a deterrent for attackers, security policies are adopted such as system hardening and intrusion detection systems.

Once a vulnerability has been exploited, specific adverse actions can be performed, such as:

- Denial of Service (DoS) on an individual machine/device, a group of devices or an entire sub-network, inside a SCADA network (DoS attacks are considered the easiest type of attack to launch);
- Software infected with malware with the aim of disrupting the performance of the network and/or the machines/devices on the network;
- Changes to the software or modifications to the configuration settings;
- Spoofing system operators and/or devices on the control network (This is the most difficult action to execute but would provide the adversary with the most capabilities);
- Changes to instructions, commands (same difficulty as above): Protocol manipulation, vulnerability exploitation and MITM attacks are among the most popular ways to manipulate insecure protocols, such as those found in control systems.

Figure 3 illustrates a typical cyber security protection system [4]. The system protects the cyber-infrastructure and combats threats at two levels: 1) at network level: "network based defence systems", and 2) at host level: "host based defence systems". Network based defence systems control the network traffic by network firewall, antivirus, spam filters and network intrusion detection techniques, whereas the host based defence systems control the data flow in a workstation by host firewall, antivirus and host intrusion detection techniques.

Models

We represent SCADA & corporate network under the occurrence of three different kinds of cyber attacks:

1. Malware injected into a specific device of corporate network, which spreads throughout the corporate network and SCADA devices up to disconnect the communication between SCADA Control Centre and its RTUs.
2. DoS attacks, in which a malicious agent exploits the weakness of network protocols to flood a specific SCADA & corporate network device, with the aim of saturating the bandwidth of the carrier among SCADA Control Center and its RTUs.
3. MITM attacks, where an attacker intercepts the traffic between two SCADA/corporate network devices and then injects new commands/information that override the original ones.

Malware propagation

The malware injection model is based on SIR (Susceptible, Infected, Resistant) mathematical formalism, for disease spread over individuals [5]. To represent SCADA and corporate network we have got a SIR net, described by a graph, where each device is a node and there is an arc whenever two nodes can communicate with each other [6]. The virus infection is the malware. A node can move from S, the susceptible group, to I, the infected group, when it comes into contact with an infected node. What qualifies a contact depends on the virus. Each infected node contacts the neighbour nodes in each step of time. Each contact may not result in the transmission of the virus, only a percent of the contacts result in transmission. For each j node (j=1,…, N), we define dj as the number of the neighbours of the node j, of which the fraction α may result infected; so, we assume that the virus spread itself, every time step, on a fraction $\beta j = \alpha \cdot dj$ of the nodes.

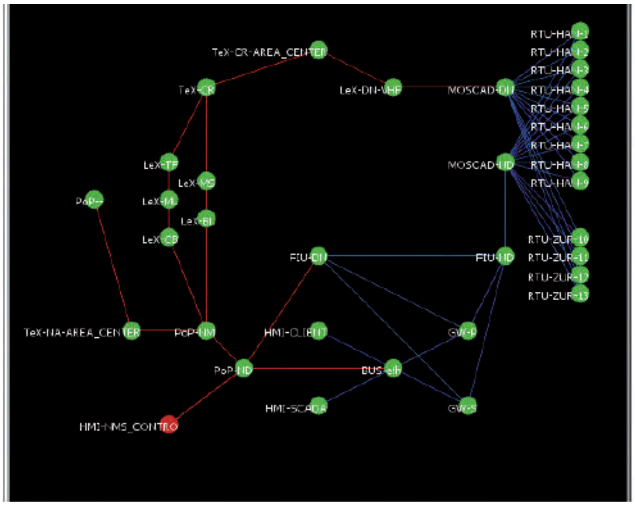


FIGURE 4 The infection starts on an NMS device of corporate network

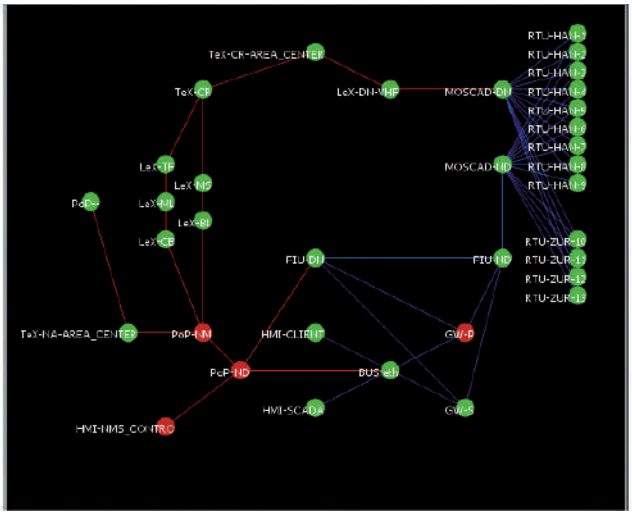


FIGURE 5 The infection spreads on corporate network and SCADA devices

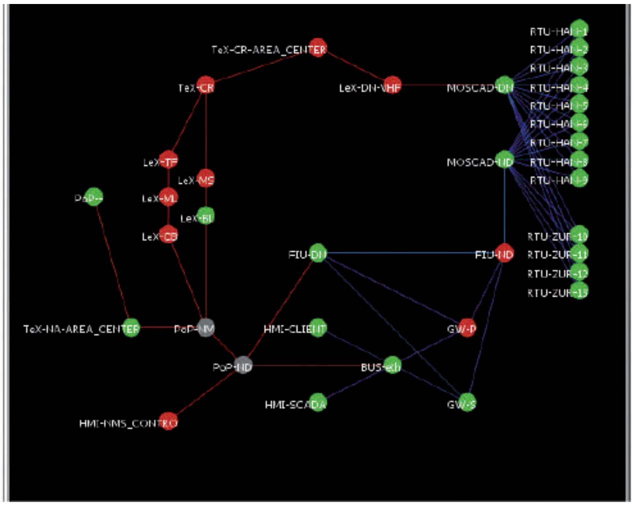


FIGURE 6 SCADA operator loses grid Observability

We justify such an assumption thinking of dealing with a stealth virus. A stealth virus does not infect nodes too much each time, since otherwise it could be more easily detected, for instance, looking at the increased traffic value. Moreover, we assume that each node has a different probability to contract the virus: γj. The virus doesn't disappear after a certain period of time, but just after periodically running the antivirus or after maintenance operations, kj is the rate of the antivirus scan. Depending on the virus, there is the possibility that the antivirus can find it and know how to remove it, ϕj is that probability. At each point of time, we have three groups of nodes and a specific numbers of nodes in a group. We have used NetLogo to create the model, set SIR variables and represent the occurrence of a cyber attack on a corporate network device (Network Management System). NetLogo is an agent-based modelling tool for simulating natural and social phenomena. It is particularly well suited for modelling complex systems developing over time. In our model, malware spreads throughout the corporate network and SCADA devices until it disconnects the communication between the SCADA Control Centre and the RTUs. We assume that the security polices of SCADA and corporate network are dependent upon the criticality of their devices. We use the following variables:

- *Alfa*: it is the spread value and it is a measure of how many neighbours are reached by the virus infection. Its range is (0, 100) %.
- *Antivir-check*: it indicates how many time units are needed to perform an antivirus check (or everything that can help to find a malware). Its range is (1, 365) days.

- *Virus-spread-time*: the virus can spread itself along the network at various rates. We assume that an infected node may infect just a fraction of its neighbours. Its range is (1, 365) days.

Figure 4 shows the screenshot, at the time t = 0 , of the SIR model. The infection starts on the Network Management System device of the corporate network (Fig. 2), named HMI-NMS_CONTRO in Figure 4. Along the infection spreading, each node of SIR model can be in one of the three states: Susceptible (*S*): the node is healthy (in green colour) and it can be infected by a malware; Infected (*I*): the node is infected (in red colour): at some rate it can infect neighbour nodes; Recovered (*R*): the antivirus scan has successfully removed the infection (in gray colour).

The links among corporate network nodes are depicted in red colour while the links among SCADA nodes are depicted in blue colour.

According to the modelling assumptions on the infection spreading, the virus propagates throughout PoP-ND and PoP-NM devices (respectively, at time step=1 and at time step=2) and, in turn, on the GW-P device (at time step =4) of the primary SCADA Control Centre-RTU connection (see Fig. 5). Then the virus spreads on LeX-CB and FIU-ND (time step= 5). The infection of the FIU-ND node causes the primary connection between the SCADA Control Centre and the Remote Terminal Units to get out of service. At such a stage, the SCADA operator still has a full observability and operability of the electrical grid of Figure 1, by means of the secondary communication between the SCADA Control Centre and the RTUs. At time step = 52, the virus also infects the TeX-CR node. At this stage (Fig. 6), the SCADA operator completely loses the observability and operability of the electrical grid of Figure 1. If a permanent electrical failure occurs on the grid, the SCADA operator cannot run the FISR service remotely.

DoS and MITM attacks

DoS and MITM attacks are specified in terms of attack parameters, attack initiation sources, attack targets. Specifically, attack initiation sources fully cover SCADA & corporate devices and even external devices connected by means of the internet. Attack targets have been chosen to cause a maximum number of damaged SCADA devices as a consequence of a successful attack on a single device.

Different indicators of expected consequences of a DoS or MITM attack have been investigated. Any attack may result in the loss of view and of control of the RTUs (and thus of the electrical grid) from SCADA Control Center. In our models we measure the following numeric indicators of SCADA performances on the attack occurrence:

- *LoV*, Loss of View: the SCADA Control Center cannot receive packets from the RTUs;
- *LoC*, Loss of Control: the RTUs cannot receive packets from the SCADA Control Center;
- *DPR*, Dropped Packets Rate: how many packets are missing on the network;
- *TTBP*, Transmission Time Between two Packets;
- *RTT*, packet Round Trip Time: composed by TCP transmission time plus ACK transmission time;
- *Packets routing*.

DoS attacks have been performed with the aim of saturating the bandwidth of the carrier used for the communication between the SCC and its RTUs. The MOSCAD front end of Figure 2 has been chosen as an attack target. The main parameters of the DoS attacks have been specified in terms of packet size, interval between packet transmission, number of packets sent during the attack, the protocol of the flood attack.

The main characteristics of the MITM attacks are as following:

- the attacker intercepts the traffic;
- once the traffic is intercepted, the attacker injects new commands/information that override the original ones. The injection occurs by means of packets between the SCADA Control Center and the victim RTU, with the same format of the normal SCADA packets, but with a higher frequency. The rationale is that a higher frequency of the MITM packets facilitates the overriding of normal SCADA packets;
- the attacker does not modify the payload of normal SCADA packets;
- the attacker connects to SCADA devices or corporate network devices through an Ethernet cable at the same speed of the Ethernet of the reference scenario;
- when the attacker intercepts the VHF communication, (s) he uses a VHF antenna, the propagation time between MOSCAD and MITM and from MITM and RTU is halved.

Again here, the MOSCAD front end of Figure 2 has been chosen as an attack target. Particularly, MOSCAD-DN when the attack comes from the corporate network and SCADA is working on the alternate path; MOSCAD-ND when the attack come from an external devices connected to SCADA system by means of the Internet.

To evaluate the attack consequences on SCADA's performances, we have considered the following numeric indicators of the MITM attack:

- *LoV*, the SCADA Control Center receives false information/data from MITM attacker. The consequent false observability of the Power grid from the SCADA Control Center may induce a tricky behaviour by the SCADA operator.
- *LoC*, the RTU receives false commands from the MITM attacker instead of the SCADA Control Center.
- Change of *Packets routing*.

Also a slight variation of *TTBP* and *RTT* has been expected

To predict the above indicators, we have built and run an NS2 model of SCADA & corporate network under cyber attacks, according to the schema in Figure 2 and the cyber attacks specified above. Table 1 summarizes the main parameters of DoS attacks on the SCADA system and their impact on SCADA performances. Particularly, the first four lines specify the attack parameters: source, destination, start and end time of the attack. The following four lines report the consequences of the attacks, as measured by the NS2 model: Loss of View (*LoV*), Loss of Control (*LoC*), maximum and minimum values of the Round Trip Time (*RTT*) during the attack, missing packets (*DPR*). Also, the simulation time and computation time are reported in the last two lines. Computation time grows from 15 to 21 minutes.

Figure 7 shows, as an example, the "travel times" of SCADA packets to RTU-1, under four phases of a DoS attack coming from LeX-BL.

The messages between the SCC and RTU-1 are differentiated by colour: black for commands from the SCC to RTU-1; blue for ACK from RTU-1 to the SCC; red

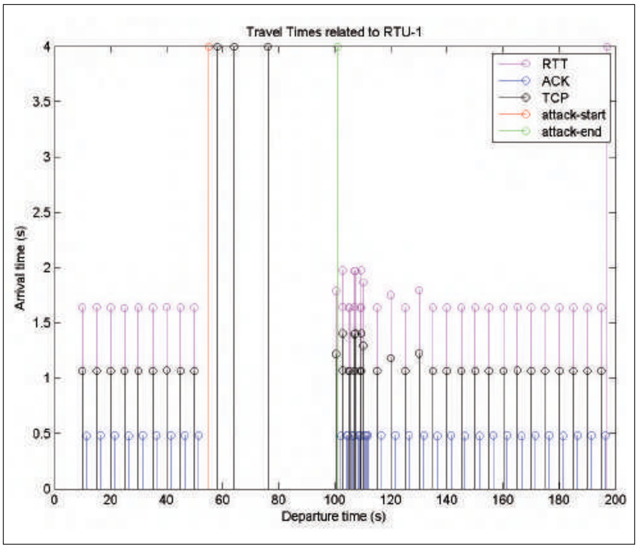


FIGURE 7 Arrival times (TCP, ACK and RTT) of SCADA packets to RTU-1 under a DoS attack

Attack source	PoP	TeX-CR	LeX-BL	Internet
Attack target	MoscadDN	MoscadDN	MoscadDN	MoscadND
Start time [sec]	55	55	55	55
Stop time [sec]	101	101	101	101
LoV	NA	NA	NA	0/17
LoC	57/57	57/57	57/57	59/76
RTT Max/Min [sec]	Inf / inf	Inf / inf	Inf / inf	Inf/ 1792
DPR	57/57	57/57	57/57	59/93
Simulation time [sec]	200	200	200	200
Computation time [min]	21	15	17	15

TABLE 1 Simulated DoS attacks on SCADA system

for the start time of the flood attack (55 s); green for the end time of the flood attack (101 s); magenta for the RTT of the exchanged packets. In Figure 7, the arrival times of packets which take an infinite time to arrive to destination are shown with a saturated arrival time of 4 sec., that is the upper border of the figure. Four attack phases can be distinguished:

1. Before the attack: SCADA packets flow from the SCC to RTU-1 and come back normally. RTT, TCP and ACK travel times are regular.
2. During the attack: the flood starts to increase the occupancy of all the buffers of the devices flooded by the attack, until they are saturated.
3. Soon after the attack: there is a tail. SCADA messages go in de-synchronization. That is due to the fact that the saturated buffer is emptied at a rate that is different from the nominal packet transmission rate; along the tail, packets are transmitted at lower intervals than the nominal ones.
4. Return to nominal conditions: flood problems end and the operative conditions come back to nominal ones.

Table 2 shows the computational time and all the traversed devices in communication between the SCC and RTU-2, along the phases of a MITM attack, which occurs between MOSCAD-ND and RTU-2. For each row of the table, the first bullet shows the route taken by SCADA packets from the SCC (n. 27) to RTU-2 (n. 5); the second bullet shows the opposite route from RTU-2 to the SCC. The MITM node (n. 38) is bold-highlighted and underlined. The relationship between numbers and devices of the SCADA and corporate network is shown in the last two columns, where the MITM node (n.38) is not included. These very simple results show the change of the packet routing, in case of MITM occurrence in the network.

Impact of cyber attacks on the electrical grid and customers

In a situation in which a permanent electrical failure of the power grid occurs and the SCADA operator cannot act remotely or can act with delay as a consequence of any of the above cyber attacks, a large portion of the power grid customers can be de-energized.

Table 3 summarizes the values of FISR response time and the percentage of the affected power grid customers. Three different operative conditions (cases) of SCADA & corporate network have been considered: case 1) nominal conditions of SCADA & corporate network under initial infection spreading; case 2) the outage of the primary path between the SCC and the RTUs; case 3) On outage of the primary path between the SCC and the RTUs, a successful cyber attack (Malware, or DoS, or MITM) causes the back-up connection between the SCC and the RTUs to get out of service; in such a case the operator loses view and control of the grid. Three different locations of the permanent electrical failure on the grid have been assumed: i) *failure in an initial section of the grid* (bounded by the feeding substation and its closest RTU): the loads of failed sub-grid are energized by the other substation until the manual repair, that restores the initial configuration of the grid; ii) *failure in an intermediate section of the grid* (bounded by two RTUs): the loads into this section are isolated, the loads bounded by the failed section and the tie switch are powered by the other substation until the manual repair, that restores the initial configuration of the grid; iii) *failure in a terminal section of the grid* (bounded by the RTU and loads): the loads of the failed section are isolated until the manual repair, that restores the initial configuration of the grid.

The first row of the table reports the location of the

Computational time:	4 sec	Device	Device number
Traversed devices before the attack	• 27 34 29 1 3 5	FIU-ND	1
	• 5 3 1 29 34 27	MOSCAD-ND	3
Traversed devices during the attack	• 27 34 29 1 3 **38** 5	RTU-HAN-2	5
	• 5 **38** 3 1 29 34 27	WIZCON SCADA	27
Traversed devices after the attack	• 27 34 29 1 3 5	GATEWAY PRIME	29
	• 5 3 1 29 34 27	BUS Ethernet	34

TABLE 2 MITM attack between MOSCAD-ND and RTU-2

Failure section		Initial	Intermediate	Terminal
Response time	case 1	18.4	34.8	29.1
[sec]	case 2	18.6	35.2	29.4
	case 3	> simulation time	> simulation time	> simulation time
affected customers	Before FISR	46.6	26.6	26.6
[%]	after FISR	0	0	6.6

TABLE 3 FISR response time and % of affected customers

permanent failure that requires the activation of FISR. Row 2 reports FISR response time in seconds, distinguished in case 1, case 2 and case 3. In case 3, the SCADA operator completely loses the observability and/or controllability of the power grid. The percentage of the affected customers depends on the section of the grid in which the failure is located. Failures in the initial section of the grid affect a higher percentage of customers. In the case of a failure of the terminal section of the grid, there is a percentage of customers out of power service till the manual repair of the failure of the grid has been completed. The outage duration of the affected customers, in cases 1 and 2, corresponds to the FISR response time plus the manual repair time, when needed. The manual repair time is needed in case of failure in a terminal section of the grid. In case 3, FISR cannot be activated remotely by the SCC and the outage duration corresponds to the manual repair of the permanent failure of the grid.

Conclusions and future work

This work, as far as we know, presents two main novelties with respect to the state of the art: a) the representation of different types of cyber attacks and their propagation on an actual SCADA & corporate network; b) the modelling process of cyber attacks and their impact on technological networks is supported by two heterogeneous tools: NetLogo, focused on malware propagation, and NS2, which computes the impact of cyber attacks on the quality of service of SCADA and its electrical grid. However, the modelling activity presents limits in representing cyber attacks. To overcome such limits we are currently investigating the use of a hybrid test bed [7] to conduct cyber attacks on SCADA and to analyze their consequences on SCADA itself and on the electrical grid. The hybrid test bed is based on the coexistence of actual, virtualized and modelled systems and devices and is intended to: i) reproduce the electrical grid, its SCADA and the corporate network; ii) conduct the three, previously described kinds of cyber attacks on SCADA and the corporate network: Malware spreading, Denial of Service (DoS) and Man in the Middle (MITM); and eventually iii) compute numerical indicators of attack consequences.

Ester Ciancamerla, Michele Minichino, Simone Palmieri, Tatiana Patriarca
ENEA, Technical Unit for Energy and Environmental Modeling - Computing and Technologic Infrastructures Laboratory

Benedetto Fresilli
ENEA, Technical Unit for Nuclear Fission Technologies and Facilities, and Nuclear Material Management – Engineering Simulator Laboratory

references & notes

[1] I. Ahmed, S. Obermeier, M. Naedele, G. Richard, 2012, “Scada systems: Challenges for forensic investigators” in IEEE Computer, 12/2012, 42-49 45(12).
[2] E. Byres, D. Lissimore, N. Kube, 2006, “Who turned out the lights? - security testing for SCADA and control systems”, in CanSecWest,, Vancouver, British Columbia, April 2006.
[3] IEC 60870-5-101 Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks.
[4] S. Dua, X. Du, 2011, “Data Mining and Machine Learning in Cybersecurity”, Boca Raton CRC Press.
[5] T. Tassier, 2005, “SIR model of epidemic” in Epidemics and Development Policy, Fordham University NY.
[6] E. Ciancamerla, M. Minichino, S. Palmieri, 2012, “On prediction of QoS of SCADA accounting cyber attacks”, Probabilistic Safety Assessment and Management Conference (PSAM11) and the Annual European Safety and Reliability Conference (ESREL 2012).
[7] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, X. Yu, 2009, “Building a SCADA security testbed”, in Proceedings of the Third International Conference on Network and System Security, 357–364.

Security e operazioni subacquee: i sistemi autoorganizzanti

Lo studio presentato in questo articolo è il risultato di un progetto finalizzato alla messa a punto e realizzazione di una nuova tecnologia marina, adatta all'uso in missioni di ricerca e salvataggio di naufraghi, protezione civile e navi militari contro attacchi terroristici, nonché alla ricerca e identificazione di congegni esplosivi pericolosi. La fusione del concetto di swarm intelligence con quello di reti di comunicazione multihop è la risposta al coordinamento durante operazioni subacquee complesse. La supervisione umana in tempo reale (in-the-loop) può essere valorizzata migliorando le prestazioni di comunicazione e ridefinendo il concetto di teleoperazione. L'elevata efficienza che la comunicazione può raggiungere rende il sistema particolarmente adatto per l'esplorazione di vaste aree in tempi brevi, come in operazioni di salvataggio in alto mare quando i tempi di sopravvivenza dei naufraghi possono ridursi a pochissimi minuti. Un prototipo swarm è attualmente in fase di collaudo.

Underwater security: Self organising systems

The study presented in this paper is the result of a project aimed at the development and realization of a novel marine technology, suitable for missions like search and rescue of people at sea, protection of civil and military ships against terroristic attacks, and search and identification of dangerous explosive devices. The fusion of the concepts of swarm intelligence and multihop communication networks is the answer to the coordination in complex underwater tasks. Human in-the-loop supervision can be exploited increasing communication performances and redefining the teleoperation concept. The high efficiency that communication can reach makes the system especially suitable in exploring large areas in short times, as in deep-water rescue operations, when the survival time of people lost at sea can be limited to very few minutes. A swarm prototype is currently under testing.

DOI: 10.12910/EAI2014-94

■ *C. Moriconi, R. Dell'Erba, S. Betti*

Introduction

Life is a continuous challenge to man's adaptation to the environment. The new paradigms created by the human science for artificial beings must face the same problems.
Along with this development philosophy and looking at the sea as one of the most promising environments in terms of humankind's economic expansion, ENEA

■ Contact person: Claudio Moriconi
claudio.moriconi@enea.it

tried to improve the current capabilities offered by the present AUV (Advanced Underwater Systems) technology relevant to mobility, perception and communications. We chose to follow the potential offered by the multi robot systems along with the philosophy of the swarms proposed by Reynolds [1], with substantial innovations on the paradigms of collective intelligence and sensing.

One of the needs is to efficiently control a high number of vessels with a central control console, coping also with the need to integrate and summarize the data coming from many different swarm elements. Another target is the system adaptivity to environmental modifications affecting communication, whether inter-individual or with the supervisor. These aspects are both related to the physical communication channel and to the geometrical distribution of the multi robot system.

The research we are carrying out at ENEA, supported by a large end-user consensus and by national projects like Harness aims at overcoming both limitations by means of an intelligent spatial distribution of transmission nodes. The project is aimed at the design of a swarm endowed with an internal intelligent architecture characterized by a close synergy between communication and geometrical/dynamical control of the swarm itself.

This paper is devoted to the role that underwater robotic teams can play in ensuring security conditions to critical infrastructures, ports, and ships. An analysis is also carried out on the high critical tasks of search and rescue following shipwrecks. Within the Harness project, funded by IIT and internally co-funded, ENEA developed a first 4-vessel swarm currently under testing.

Security needs in marine areas

Large water surfaces of Oceans and Seas have played a critical role in all the human history.

Currently the economic activities involving seas are ranging from communications (i.e., underwater cables joining continents), to large and heavy transportation, energy (offshore platforms, oil and gas terminals), food fish and farming, tourism, military actions.

Practically each one of these activities is potentially subjected to natural, military or asymmetric threats and the most critical targets, some of them involving the security of whole nations, are often not adequately protected.

Special attention is requested by end users to the protection of ships, critical infrastructures, ports, etc.. against passive (i.e., mines) and active threats (underwater attacks by scuba divers), and to the rescue of people fallen at sea. What makes robotic swarms especially useful in security actions is their capability to fill and control large volumes of water by means of a network of cooperating sensors, and their capability to move in the most interesting zones, increasing density where it is needed the most. They are also easily transportable and deployable in a small or large number of vessels.

Recent studies have been carried out by end users on applications relevant to the protection of large critical infrastructures, customised according to the features and the peculiar characteristics of our system and playing the role of second protection level. In these schemes the first level is accomplished by fixed multiphysics antennas (surface radar, underwater sonar, optical sensors, etc.) that gives a continuum picture of the surrounding environment, with a relatively high possibility of false alarms.

When an alarm is detected a swarm or part of it can be sent to intercept the alarm source(s) and to check its real threatening potential. The interception swarm must be relatively wide, fast and continuously connected to the Command and Control Room to obtain the precise position of the threats detected by the antennas of surveillance sensing system.

Currently ENEA has been called to participate in national projects for ensuring the security of sensitive infrastructures by means of this technology.

Ports surveillance

This application comes from the need to avoid intruders from taking advantage of the large traffic of a port to carry out threatening actions using explosive, radioactive materials or biological attacks.

Usually actions of this kind are monitored by surface sensors, like surface radars and optical surveillance devices, yet such systems have a limited alarm capability when the threats are brought by divers. Several scenarios have been studied for asymmetrical attacks: some of them refer to the transportation of divers to a distance suitable to reach the target by underwater swimming. Acoustical barriers can offer adequate protection, but their main drawback is their need for frequent maintenance to ensure their effectiveness. This is a considerable cost and they cannot be managed in a flexible way since deployment and withdrawal operations are also expensive and time consuming.

The use of mobile surveillance nodes can represent an effective alternative to these systems. They offer the possibility to be easily brought into operation only when there is an actual need, in very short times and without any external evidence of the operation. The alert system can be operated using different approaches, ranging from acoustical barriers (passive or active) to visual alarms and magnetic alerts.

In addition to their security functions, these tools have also been considered by large European ports (Le Havre, Rotterdam, Marseille) as a practical device to explore the conditions of the vessel of large ships, within their loading and unloading operation, without having to recover them into a hangar or to realize fixed sensing equipment in every dock.

The preliminary analysis has also characterized the fixed equipment as an expensive approach, considering the maintenance needs and the fact that only a limited number of docks could be exploited for this use (almost half of the docks in a large port are usually under maintenance conditions and, therefore, not suitable for ship docking).

Requests for detection barriers and rescue operations

The capability to search and detect bodies at sea is a surprisingly important request. Some years ago our group has been advised about the importance of such a capability during a preliminary presentation of the ENEA's underwater swarm project later named Harness.

The interest was in the threat represented by the possibility for silent diving intruders to overcome all the ships' electronic defenses thanks to the modern scuba equipment. Acoustical barriers cannot be deployed in all the cases, especially when ships are anchored outside the ports and, on the other hand, the classical sonar equipment cannot be effective in most cases since the human body, having a density very close to that of water, often absorbs the sonar beams and suitable suits can further decrease the tiny echoes. The capability to deploy an acoustical network of protecting mobile nodes, based on the lacking of transmitted sonar pulses rather than on their reflection, seemed therefore greatly estimated by the end user.

For an analysis of some possible approaches to the sensor coverage the theme has been widely treated and we can refer to the works of Liu [2] and Barr [3]. The concept of a safety equipment deployable in case of needs turned out to be much wider than in the mentioned case and urged our group to study the problem more deeply.

The chance of survival for people fallen at sea is quite low, especially in cold climates, and decreases quickly if the body is not immediately recovered. When shipwrecked people start losing their forces and are no longer able to continuously sustain themselves on the surface, the detection possibilities become quickly worst and worst.

A mobile swarm like the one discussed for ships' protection can become a powerful tool also for the rescue of people lost at sea. The combination of two resources of such a system, the capability of efficiently apply a volumetric detection, and the capability to keep trace of the explored volumes can be considered an important advantage in many cases. Also mine fields can be efficiently detected and then removed with the appropriate tools by means of this detection method. Despite the fact that they are intrinsically more detectable by sonar ships, there are modern mines protected by means of phonoabsorbent surfaces.

General considerations on the ENEA's project

The underwater environment is strongly variable from a communication point of view, depending on salinity, turbidity, presence of dissolved substances that change the color and transparency in different optical bands.

Therefore communications can take place with greater or lower speed in the optical or acoustical channels, with different delays, attenuations, angular distributions of the radiated power. A multi-body system, can react to these modifications modifying both the parameters of the transmission "equipment" and the physical dispersion/geometry of the system itself. If the mission of the system demands for a greater dispersion to maximise the volume to be explored, the communication bandpass could be reduced and the main stream of the information could be switched from the optical to the acoustical mode. Natural examples are in the following Figures 1 and 2, representing a couple of typical situations.

Common mode behaviors often generate peculiar geometrical shapes as an answer to survival challenges. These behaviors are the result of learning processes that are partially carried out during the life of the swarm [12] and partially carried out during the evolution of the species through a genetic selection process. Some reference shapes have been defined as a reply to the needs of selected applications in Figures 3, 4 and 5. The global control architecture is built around three basic elements: the supervisor goals, the inter-nodal communications, the priorities of each single individual (typically collision avoidance). The behavior and the swarm configuration will change

FIGURE 1 Adaptation of a bird swarm to environmental need (food hunting)

FIGURE 2 Cylinder shape obtained by the internal rules of a swarm, usually as a reaction to a threat by a hunter

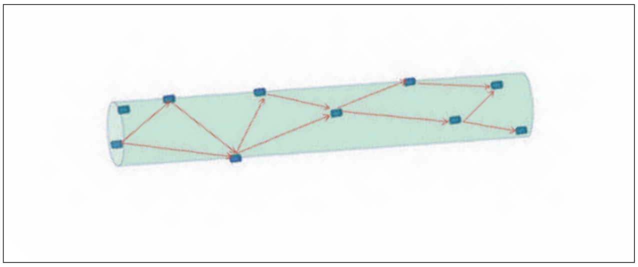


FIGURE 3 The "pipe": when the communication is the main objective of the geometrical shape to transport data on long distances at high data rates

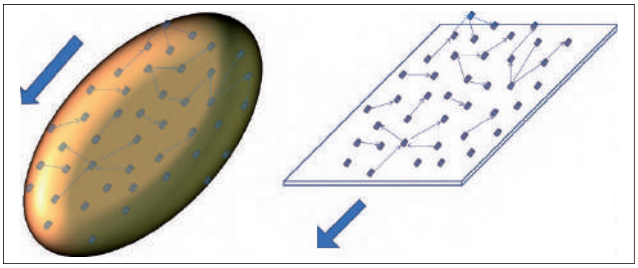


FIGURE 4 - 5 The "plane", especially suitable to carry out fast and parallel survey operations of the basements. Especially aimed at allowing a high rate exchange of information among the nodes. "Ellipse" is a quite typical shape used in fish schools, typically aimed at giving the most impressive "footprint" to possible predators, but it is also the result of the dynamical processes of arrangement of the schools themselves

depending on the assigned tasks, the survival risk associated to the operation of each robot and the risk relevant to the loss of connection of each vessel with the multi-body system as a whole.

Previous studies to address the formation control and coordination can be found in [4] and in the basic work of Khatib [5].

Research challenges and first steps

The concept of a multi-body system that behaves, to some extent, as a single entity is in line with the approach followed by nature's evolution. Societies, Swarms, Colonies down to the case of an individual, seen as an association of specialized cells, are all different forms of multi-body systems where the specific nature of the association is determined by the optimal answer to environmental conditions.

The following basic challenges are addressed:

a) Overcoming the problem of low data transmission bandpass inside marine water;
b) Drastically improving the monitoring capability for tasks requested in sea coastal areas (pollution and biological controls, intrusion surveillance, rescue operations);
c) Getting an easy and fast supervised control by a human operator, at a high-level decision capability.
d) Optimizing the system behavior in different environments to improve its robustness and reliability;

In the following, the facility realized for the preliminary tests is shown (Fig. 6).

The final vessel has been designed in the ENEA's labs after a long time spent to optimize all the economically relevant components. Our final objective was to achieve a vessel, big enough to transport a minimum amount of sensoriality and to have a reasonable autonomy, but as cheap as possible to put together a realistic swarm.

From the assembly drawing, after further optimizations on the electronics, we realized the first prototype of VENUS (see Fig. 7).

Currently 4 VENUS vessel prototypes have been realized, the single vessel testing is in progress (Fig. 8) and the first swarming tests are expected to be

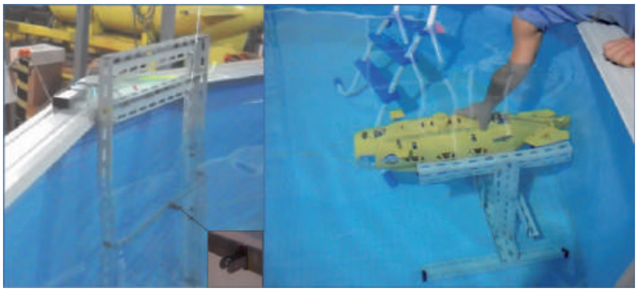


FIGURE 6 Commercial low-cost platform in the ENEA's testing pool facility

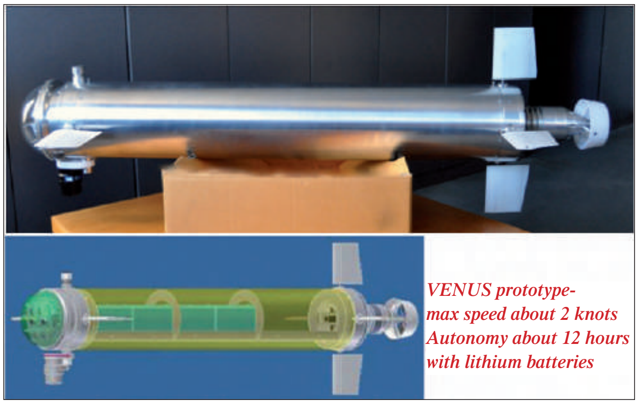


FIGURE 7 First prototype of VENUS

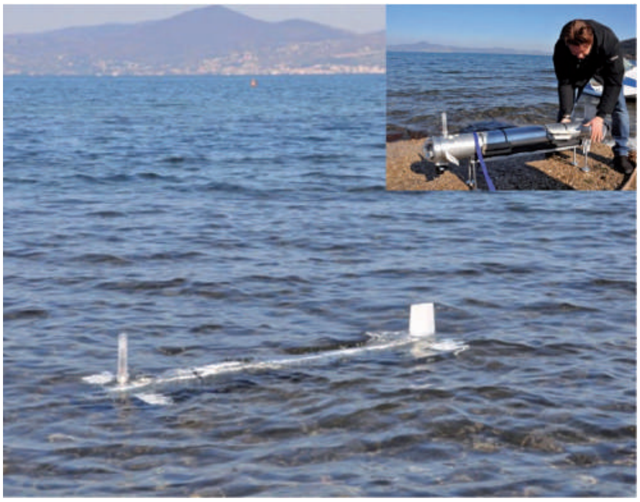


FIGURE 8 Venus testing at Bracciano's lake

performed by the end of the current year. Incoming projects should make the realization of large functional swarms possible.

The algorithmic work carried out so far has led to the following results in the simulation test-bed:

- to maintain short distances among all the swarm members;
- to change the swarm geometry with the specific task, flat distribution to explore wide surfaces,
- to simplify the remote control interaction, treating the whole system as a single composite body.

Four technology areas are envisaged as key elements of the architecture: Communication, Control, Localisation, Teleoperation.

Communication

Most of the intelligent swarm functions are based on performances of the communication channel.

The underwater environment strongly limits the practical signals that can be exploited [9]. We considered the following different categories:

a) acoustical active signals,
b) acoustical passive signals,
c) electromagnetic (optical) active signals,
d) electromagnetic (optical) passive signals,
e) electromagnetic active signals (only for surface communication).

In the following, some issues of this critical subject will be discussed.

The underwater swarm is a wireless network of mobile nodes able to cope with different needs, depending on the physical arrangement of the node geometry. We envisaged at the least:

a. the need for a fast data transmission rate on relatively long distances (High Speed Transmission); a pipe geometry, small distances and slow movements are the conditions to adopt sensitive protocols like PSK and QAM for video streaming;
b. the need to increase the swarm internal data exchange (High Swarm Bandpass) to allow processing like the fusion of data from the sensors of many vessels on the same target;
c. the need to maintain a disperse swarm configuration to accomplish wide area monitoring tasks (Wide Area Surveillance).

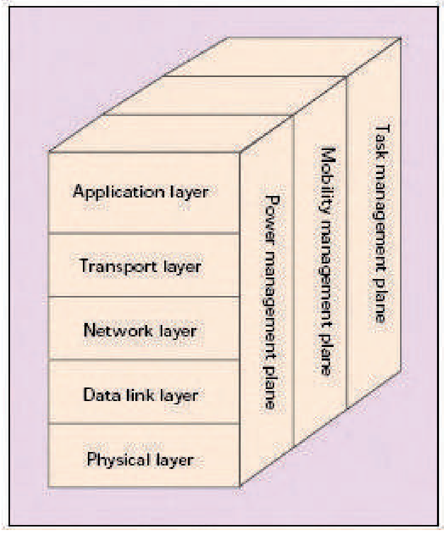


FIGURE 9 Protocol Stack for Harness project

Transmission protocol aspects

Recent advances in communications and electronics supplied low-power, multi-functional sensors and control nodes spread in integrated networks. These nodes consist of sensing, controlling, data processing, and communicating components.

Realizing these sensor network applications requires ad hoc networking techniques, especially underwater, where particular difficulties can be found. The protocol stack combines power and routing awareness, integrates data with protocols, communicates power efficiently, and promotes cooperative node efforts. It consists of the traditional layers: physical, data link, network, transport, and application layer as in Figure 9.

The "vertical" layers share information among all the traditional layers in order to improve the performance of the sensor & control nodes. The power management plane manages the node power. The mobility plane detects and registers the movement of nodes, so that a route back to the user is always maintained, and the sensor nodes keeps track of the neighbor sensor nodes. The different data categories involve basically different requirements in terms of transmission range, priority, speed and allowed BER (bus error) so much that the category will also affect the MAC (medium access control) and even the swarm configuration.

We basically consider four types of messages:

1. "sync" messages, i.e. the heartbeat of the system;
2. "sensorial" data, giving a picture of the environment as perceived by the many sensors of the swarm;
3. "supervision" messages, that are mainly addressed to the supervision station; they can include, for instance, video streams and commands;
4. "service and intelligence" messages, addressed to the other nodes to carry out system services like alerts of many types.

Control

The control system for 3D swarms, also in the underwater environment, is already a well-treated topic in literature; starting by the fundamental work of Bonabeau [8], several authors tried to cope with different aspects of the control problems like in [4, 8, 9]. We considered the ability of the swarm to react to the environmental stimuli and to mission modifications managed by several composite control layers of the Intelligence subsystem (Fig. 10).

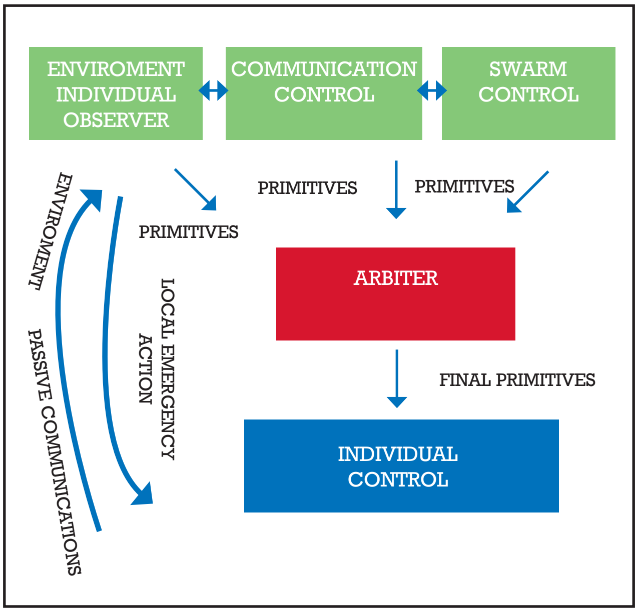


FIGURE 10 Principle control scheme

The three main layers that we choose to introduce to achieve this result are:

- the Communication control,
- the Swarm control,
- the Individual control.

In addition a fourth layer, the Arbiter, solves conflicts that can arise among the previous levels:

The Intelligence architecture is based on a sort of MIMD architecture where each individual has the same processing hardware and the full potential processing functions.

Communication Control

Communication is a part of the intelligence of the system able to give commands to the Swarm, just as the other parts of the Intelligence Subsystem.

Communication Intelligent Layer senses progressive degradations of data transmission efficiency and obtains by SC data of the environment adopting correcting measures, like the physical modification of the Swarm rule that controls the distance among the vessels. A classical discussion can be found in [6, 7], whereas a reference research has been carried out and recently presented [11, 13].

Swarm Control

The Swarm Control generates the primitives sent to the Individual Control for the planning of the trajectories.

A typical "primitive" rule could be: "bring the mean distance from your neighbors to less than 5 meters". This kind of rule (the Primitive) has no effect on the trajectory of an inner swarm individual since it lacks additional information. Other inputs are required and the rule system quickly becomes a relatively complex system. In this case a Direction Priority is required to address the Left/Right or Up/Down and the relevant versus.

Individual Control

Individual Control (IC) could be seen as a "classical" AUV control, able to carry out functions like path planning, collision avoidance, absolute and relative speed control, and so on.

Individual Control solves the problems and the conflicts relevant to the rules application like the obstacle collision avoidance. In this case a useful strategy could bring to a separation of the school in two or more parts and the rejoining could generate conflicting situations [4, 10].

Arbiter

The Arbiter function represents a concept introduced to cope with the conflicts among different needs of the system and with the layers that take these needs into account.

Localisation

A living creature is typically aimed at fighting for food and standing by in the most convenient environment for the survival of the individual or of the group. Therefore in most cases it is more appropriate to talk about localization of the creature or Group inside a different space (space of the food – typically sensed by smell, space of the safety – identified by sensing the occurrence of possible threats, space of reproduction areas and so on). Of course, all of these spaces have their mapping into the geographical space. Rough, Precision and Relative Localisations are three different approaches that must be obtained for an effective navigation.

Rough Localisation

It is the capability of a Swarm to sense and identify non-metric features of the environment (refer to the aforementioned food space and others). This can be useful in carrying out surveillance missions of wide areas, when a precise localization is not useful during the whole mission, but only at the time when a target is identified. A possible light and cheap sensing equipment able to collect similar information is based on passive acoustical data. Typically the marine areas are acoustically mapped on the basis of their noise footprint and a large system like the Swarm is able to recognise the area location.

Precision Localisation

It can only be achieved endowing the vessels with Global Positioning System beacons and to elect some of the individuals to the role of surface navigators. The information exchanged through the network can allow for the geographical localization of the whole school.

Relative Localisation

Advanced algorithms, coping with the classical problem of trilateration but avoiding degenerate solutions, aimed at defining the relative position of each individual in the swarm to perform a task (i.e., define a trajectory implicitly or explicitly with respect to its mass center, define a space distribution, etc.). Cameras, pressure meters, compasses or acoustic devices can supply the information needed to fix the value of the distance from each individual to another and to establish absolute values (depths, speeds, angles with respect to the earth's magnetic field).

Teleoperation

Teleoperation represents one of the main targets of the research line. In environments like Underwater and Space, where delays and transmission bandpass are an important issue, the man-in-the-loop scheme asks for particular care. The classical approach of Teleoperation, an external sequence of orders, with a metrics inside, is not the best way to cope with a Swarm paradigm. Teleoperation can be maintained in its original form (remote operation replicated as if the operator is present on the place) if and only if the telecommunication properties allow the closure of the loop with an acceptable delay with respect to on-going task.

In any other case, the remote "slave" must be endowed with an increasing decisional capability so that teleoperation and telepresence become a new form of symbiosis, a telecooperation system that ranges, without sharp steps, between the two ending points of a complete autonomy and the true teleoperation. We define "high telecooperation level" a condition close to the true teleoperation, and "low telecooperation level" the condition approximating to the autonomous operation.

Conclusions

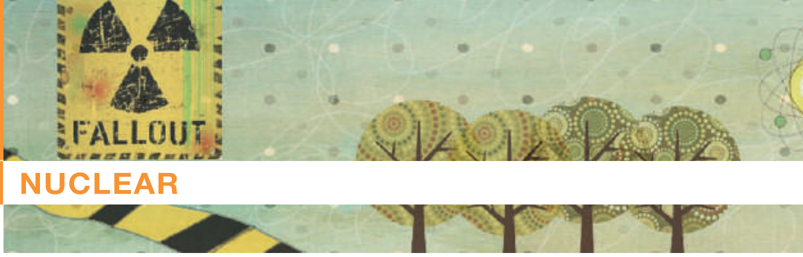
The system that ENEA is now testing has been considered as an interesting approach by many end users and in the next years the realization has been planned of some swarms to be built and tested under real operating conditions. At the same time, the more advanced functions relevant to communications, continuous connection to the surface, group intelligence and extended sensing will be developed to allow more powerful and advanced functions.

Claudio Moriconi, Ramiro Dell'Erba
ENEA, Technical Unit for Advanced Technologies for Energy and Industry - Robotics Laboratory

Silvello Betti
University of Rome Tor Vergata, Electronic Engineering Department

references & notes

[1] C. Reynolds, "Flocks, Herds, and Schools: A Distributed Behavioral Model", 1987, in Computer Graphics, 21(4), July 1987, 25-34.
[2] B. Liu, D. Towsley, , 2004, "A study on the coverage of large-scale sensor networks," in The 1st IEEE Internat. Conf. on Mobile Ad-hoc and Sensor Systems.
[3] S. Barr, B. Liu, J. Wang, 2008, "Barrier coverage for underwater sensor networks," in Milcom 2008 Proceedings.
[4] A. Fax, R. M. Murray, 2004, "Information flow and cooperative control of vehicle formations" in IEEE Trans. on Automatic Control, 49(9), September 2004, 1465–1476,
[5] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots", 1986, in Int. Journal of Robotics Research, 5(1), 90–98.
[6] E. Sozer, M. Stojanovic, J. Proakis, 2000, "Underwater Acoustic Networks" in IEEE Journal of Oceanic Engineering, 25(1), January 2000, 72–83.
[7] J. Proakis, E. Sozer, J. Rice, M. Stojanovic, 2001, "Shallow Water Acoustic Networks", in IEEE Communications Magazine, Nov. 2001, 114–119.
[8] E. Bonabeau, M. Dorigo, G. Theraulaz, 1999, Swarm intelligence : from natural to artificial systems, Oxford University Press, New York, NY, USA.
[9] I.F. Akyildiz, D. Pompili, T. Melodia, 2004,"Challenges for Efficient Communication in Underwater Acoustic Sensor Networks," in ACM Sigbed Review - Special issue on embedded sensor networks and wireless computing, 1(2), July 2004, 3-8.
[10] Y. Hanada, L. Geunho, N. Chong, 2007, "Adaptive flocking of a swarm of robots based on local interactions," in Proc. of the IEEE Swarm Intelligence Symposium, (Honolulu, Hawaii), 340–347.
[11] Z. Zhou et al., 2011, "Efficient multipath communication for time-critical applications in underwater acoustic sensor networks", in IEEE/ACM Trans. on Networking, 19(1), 28–41.
[12] C. Blum, D. Merkle (Eds), Swarm Intelligence – Introduction and Applications, Springer, 2008.
[13] M. Tabacchiera, S. Persia, C. Lodovisi, S. Betti, 2011, "Performance Analysis of Underwater Swarm Sensor Networks", in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference, 333-338.



Il processo del Nuclear Security Summit: il giro di vite

Il processo del Nuclear Security Summit (NSS) è iniziato nel 2010 in occasione del Nuclear Security Summit di Washington DC, seguito dai Summit di Seoul nel 2012 e de L'Aja nel 2014. Un quarto Summit è previsto nel 2016, sempre negli Stati Uniti. Il processo NSS ha portato all'impegno, senza precedenti, da parte di 53 leader di stato a rafforzare la security nucleare a livello nazionale e internazionale. Agli impegni di natura volontaria sono seguiti passi concreti verso la creazione di un sistema globale di nuclear security. L'autrice del presente articolo, che ha preso parte a tutte le fasi del processo NSS fin dal primo incontro preparatorio nel Settembre 2009, presenta una panoramica del processo NSS e dei risultati raggiunti, esaminando la minaccia nucleare e il contesto internazionale.

The Nuclear Security Summit process: The turn of the screw

The Nuclear Security Summit (NSS) process was launched with the Nuclear Security Summit in Washington DC in 2010, followed by the summits in Seoul in 2012, and in The Hague in 2014. A fourth summit is to be held in 2016, once again in the United States. The NSS process has resulted in an unprecedented commitment by 53 State leaders to strengthen nuclear security at the national and international levels. The commitments, of a voluntary nature, have been followed by concrete steps toward the creation of a global nuclear security framework. The author, who has participated in all phases of the NSS process since the first preparatory meeting in September 2009, presents an overview of the NSS process and its achievements, examining the nuclear threat and the international framework.

DOI: 10.12910/EAI2014-95

■ *F. Padoani*

Introduzione

Con il processo del Nuclear Security Summit (NSS) l'approccio internazionale alla security nucleare e la percezione della stessa minaccia nucleare è completamente cambiato, elevando al massimo livello politico una problematica che fino a pochi anni fa molti Paesi non apprezzavano del tutto e delegavano quasi interamente a tecnici e esperti. A seguito dei primi tre Nuclear Security Summit, molto è stato ottenuto a livello nazionale e internazionale nel rafforzamento di un sistema globale di nuclear security, che oramai è riconosciuto come un obiettivo comune da tutti i Paesi partecipanti al processo NSS.

Introduction

The Nuclear Security Summit (NSS) process has completely changed the international approach to nuclear security and perception of the nuclear threat, raising to a high political level an issue that until a few years ago many countries did not fully appreciate, delegating it almost

■ **Contact person: Franca Padoani**
franca.padoani@enea.it

FIGURE 1 The Nuclear Security Summit, Washington 2010
Il Nuclear Security Summit, Washington DC 2010
Source: http://www.state.gov/t/isn/nuclearsecuritysummit/

I Nuclear Security Summit

Washington DC 2010

Il Presidente Obama ha dato avvio al processo a Praga nel 2009, con il famoso discorso in cui esortava a impegnarsi per "un mondo senza armi nucleari", e la convocazione del primo Nuclear Security Summit a Washington DC, il 12-13 aprile 2010. Con la partecipazione di 47 Paesi, rappresentati principalmente dai rispettivi Capi di Stato, insieme alle Nazioni Unite, l'AIEA e l'Unione Europea in qualità di osservatori, si è trattata della più grande riunione di Capi di Stato mai organizzata da un Presidente statunitense fin dalla Conferenza per la fondazione delle Nazioni Unite, nel 1945. L'Italia era rappresentata dall'allora Primo Ministro, Silvio Berlusconi. I risultati di questo primo sono stati di eccezionale rilievo: per la prima volta 43 leader, tramite un Communiqué congiunto [1] e un work plan [2], hanno riconosciuto la serietà della minaccia posta dal terrorismo nucleare alla sicurezza internazionale e si sono impegnati (sebbene senza alcun vincolo legale) a compiere passi concreti per mettere in sicurezza, nell'arco di quattro anni, il materiale nucleare

entirely to technical experts. With the first three Nuclear Security Summits much has been achieved, nationally and internationally, for the purpose of strengthening the global nuclear security framework, now recognized by all countries of the NSS process as a shared objective.

The nuclear security summits

Washington DC 2010

The process started with the 2009 speech in Prague by President Obama, with a view to working towards securing "a world without nuclear weapons". He then convened the first Nuclear Security Summit in Washington DC on 12-13 April, 2010, with 47 countries, mainly represented by their Heads of State, together with the United Nations (UN), the IAEA and the European Union as observers. This was the largest gathering of state leaders hosted by a US President since the Conference for the founding of the UN in 1945. Italy was represented by the then Prime Minister, Silvio Berlusconi. The achievements were outstanding: for the first time 43 leaders, through a joint Communiqué [1] and Work Plan [2], recognized the seriousness of the threat to international security posed by nuclear terrorism. They committed themselves (though without any legal obligations) to take concrete steps *più sensibile, cioè uranio altamente arricchito (HEU) e plutonio, e di prevenirne il traffico illecito. Il Communiqué ribadisce che la sicurezza nazionale è responsabilità dei singoli Stati, ma allo stesso tempo riconosce l'importanza della cooperazione internazionale nella lotta alla minaccia nucleare.*

Seoul 2012

Il Summit di Washington si è svolto in una fase cruciale per il disarmo e la non proliferazione – la firma del trattato START (Strategic Arms Reduction Treaty) per la riduzione delle armi strategiche, la pubblicazione della nuova Nuclear Posture Review e l'imminenza della Non-Proliferation Treaty Review Conference – che ne ha influenzato positivamente i lavori e suscitato l'interesse dell'opinione pubblica. Il NSS di Seoul si è tenuto il 26-27 Marzo 2012, in un periodo di accresciuta tensione internazionale fortemente influenzata dal difficile rapporto del Paese ospitante con la Corea del Nord e dal drammatico evento di Fukushima in Giappone. Il Communiqué [3], sottoscritto dai leader dei 53 Paesi partecipanti, riconferma gli impegni assunti nel 2010 e elabora ulteriormente il tema della minaccia nucleare. A Seoul, l'Interpol si è unita come quarto osservatore. Uno degli elementi di novità è stata l'attenzione posta sulla minaccia derivante dalle sorgenti radioattive e, più in generale, dal materiale radioattivo, un aspetto che nel Communiqué di Washington era solo abbozzato. Altro elemento di novità nel Communiqué di Seoul, è stata l'introduzione di considerazioni sulla nuclear safety e sulla sua interfaccia con la nuclear security. L'allora Primo Ministro, Mario Monti, con una dichiarazione molto apprezzata sulla safety-security, ha sottolineato le specificità della situazione italiana e la questione della trasparenza, che sarebbe stata oggetto di ampio dibattito in occasione del successivo Summit de L'Aja (Riquadro 1).

L'Aja 2014

Il terzo Nuclear Security Summit ha avuto luogo il 24-25 Marzo 2014 a L'Aja, con la partecipazione dei leader di 53 Paesi e quattro organizzazioni internazionali. L'Italia è stata rappresentata dal Primo Ministro, Matteo Renzi, e dal Ministro degli Affari Esteri, Federica Mogherini. Sebbene all'epoca l'attenzione politica fosse incentrata sulla crisi in Ucraina, il NSS ha comunque riscosso grande successo.

Rispetto al Summit di Seoul, il Communiqué [4] ha posto un accento ancora maggiore sulla necessità di rafforzare la security dei materiali

to secure key nuclear material, namely highly enriched uranium (HEU) and plutonium within four years, and to prevent its illicit trafficking. While reaffirming that nuclear security is entirely the responsibility of States, the Communiqué recognizes the importance of international cooperation in fighting the nuclear threat.

Seoul 2012

The Washington Summit was held in an important phase for disarmament and non-proliferation – with the signing of START (the Strategic Arms Reduction Treaty), the new Nuclear Posture Review and the impending Non-Proliferation Treaty Review Conference – thus positively influencing its work and raising public attention. The NSS in Seoul, held on 26-27 March 2012, took place in a period of heightened international tension,

Nuclear Security Summit Seoul, 26-27 March, 2012

…

Even if safety and security are distinct issues and have been dealt with separately both at the national and international level, an integrated and coherent approach appears increasingly necessary. This applies both to the measures to be adopted and to the regulatory measures undertaken in the two sectors. The tragic accident at Fukushima Dai-Ichi bears witness to the pressing need for a coordinated approach.

Full integration is hindered by the confidentiality required in managing nuclear security information. This prevents the full transparency which, instead, is required for nuclear safety.

Further steps towards increased integration are feasible and welcome. We should reduce to the minimum the areas which require separate interventions, while ensuring a general coordination in the two fields.

As to nuclear security, the Italian legal and operational framework goes in the right direction by considering separately "active" and "passive" measures of physical protection. The bodies in charge of "passive" protection (i.e. the Ministry of Economic Development and the regulator ISPRA) are also in charge of nuclear safety. With these task assignments, conditions are in place in Italy for a coherent approach to nuclear safety and security by plant operators and regulatory authorities.

It is important, in conclusion, that national regulatory and control systems are structured in a way that the safety-security interface is adequately managed so as to ensure that all measures taken are coordinated and compatible.

BOX 1 Excerpt from the Italian Prime Minister's statement on "Nuclear Safety – Security interface" at the Seoul NSS
Estratto dalla dichiarazione rilasciata al Summit di Seoul dal Primo Ministro Italiano su "Interfaccia safety e security nucleare"

radioattivi, riflettendo la crescente consapevolezza che una "bomba sporca" potrebbe rappresentare la minaccia più concreta. Inoltre, riferendosi all'interfaccia tra safety e security, evidenzia per la prima volta l'importanza di un approccio comune nella risposta alle emergenze nucleari e radiologiche. Tuttavia, l'elemento originale di questo Summit è stata l'ulteriore elaborazione del concetto di architettura globale di security nucleare: sebbene vi sia un consenso generale sulla responsabilità nazionale in materia di security nucleare, è evidente che la security nucleare deve essere trattata a livello globale. L'architettura globale deve basarsi su strumenti internazionali ed essere rafforzata dal ruolo delle Nazioni Unite e di altri organismi internazionali, in particolare l'AIEA, ma non solo. Perché ciò avvenga, è fondamentale la garanzia che ogni paese adotti misure di security nucleare appropriate; in questo spirito, il Communiqué elenca una serie di azioni volontarie che gli Stati possono intraprendere al fine di dare assicurazioni alla comunità internazionale sull'efficacia delle misure di security nucleare adottate a livello nazionale.

Impegni nazionali e Gift Basket

I Communiqué e il Work Plan di Washington sono l'unico prodotto dei Nuclear Security Summit. Tuttavia, dal Summit di Washington ci sono stati ulteriori impegni, originariamente essenzialmente unilaterali, noti come "house gifts". Seoul ha visto l'introduzione del concetto di "Gift Baskets", cioè dichiarazioni multinazionali, il cui ruolo è stato meglio definito nei due anni

strongly affected by the difficult relationship of the host country with North Korea and by the dramatic Fukushima accident in Japan. The Communiqué [3] by the leaders of the 53 participating countries confirmed the 2010 commitments and further elaborated on the nuclear threat. In addition, Interpol joined as a fourth observer. A new element was the focus on the threat posed by radioactive sources, and more in general by radioactive material, an aspect that was only briefly touched on in the Washington Communiqué. Nuclear safety considerations and the interface with nuclear security was the other new element in the Seoul Communiqué. The then Prime Minister of Italy, Mario Monti, delivered a much appreciated statement on safety-security, pointing out the specificities of the Italian situation and the question of transparency that was to be much debated in The Hague (Box 1).

The Hague 2014

The third Nuclear Security Summit was held on 24-25 March, 2014, in The Hague, NL, with the participation of leaders from 53 countries and four international organizations. Prime Minister, Matteo Renzi, and Federica Mogherini, Minister for Foreign Affairs, represented Italy. Although political attention at that time was focusing on the Ukraine crisis, the NSS was nevertheless a great success.

With respect to Seoul, the Communiqué [4] was stronger in reaffirming the need to strengthen the security of radioactive materials, reflecting the growing awareness that a "dirty bomb'" could be the most concrete threat. Moreover, in dealing with the interface between safety and security, it highlights for the first time the importance of a common approach for emergency response. However, the original element of this Summit was the further elaboration of the concept of a global nuclear security architecture: although there is a consensus on the national

FIGURE 2 Opening Ceremony and Presidents Obama (US) and Rutte (NL) at the closing session of the Nuclear Security Summit in The Hague

La cerimonia di apertura e i Presidenti Obama (US) e Rutte (NL) durante la sessione conclusiva del Nuclear Security Summit de L'Aja

Source: https://www.nss2014.com and http://youtu.be/NNJdMMVshLs/

Name of the Gift Basket (NSS)	Gift Basket holder	Participants
Counter Nuclear Smuggling (2012)	Jordan	21 (Italy)
Forensics in Nuclear Security (2014)	The Netherlands	27 (Italy)
GICNT-Global Initiative to Combat Nuclear Terrorism	Russian Federation, US and others	Not foreseen
HEU-Free Joint Statement (2014)	US	13
In larger Security: a Comprehensive Approach to Nuclear Security (2014)	Brazil	15
Maritime Supply Chain Security (2014)	US	13
National Legislation Implementation Kit on Nuclear Security (2012)	Indonesia	30
Nuclear Information Security (2012)	United Kingdom	35 (Italy)
Nuclear Security Training & Support Centers / Centers of Excellence (NSSC/CoE) (2014)	Italy	31 (Italy)
Radiological Security (2014)	US	23 (Italy)
Strengthening Nuclear Security Implementation (2014)	US + South Korea + NL	35 (Italy)
Transport Security (2012)	Japan	5
UNSC Resolution 1540 (2012)	Canada + South Korea	33 (Italy)

TABLE 1 Gift Baskets at the Nuclear Security Summit in The Hague. Participants as of 24 March, 2014
Gift Basket presentati al Nuclear Security Summit de L'Aja. Partecipanti al 24 marzo 2014
Source: https://www.nss2014.com/

che hanno portato al Summit de L'Aja e che ora sono considerati come un contributo importante all'ulteriore rafforzamento del Communiqué.
Al Summit de L'Aja, l'Italia ha presentato il Gift Basket "Nuclear Security Training and Support Centres/Centres of Excellence (NSSC/CoE)" [5] con lo scopo di dimostrare i progressi raggiunti a partire dal Summit di Washington, continuando nel frattempo a promuovere lo sviluppo di centri di formazione e supporto / centri di eccellenza sulla security nucleare e intensificando la cooperazione internazionale e regionale. Questo Gift Basket e il suo successo possono interpretarsi come il riconoscimento degli sforzi dell'Italia nel processo NSS per rafforzare la cultura della security nucleare.
Al Summit di Washington, che ha dato una importanza senza precedenti alla dimensione umana, l'Italia si è impegnata a livello nazionale per la realizzazione, insieme all'AIEA e all'International Centre for Theoretical Physics (ICTP), della International Nuclear Security School con sede a Trieste: la Scuola ha dato avvio al primo corso l'anno successivo, nell'aprile 2011, e nel 2014 si è tenuto il quarto corso.

responsibility for nuclear security, it is clear that nuclear security has to be dealt with at the global level. The global architecture must be based on the international instruments and strengthened by the role of the UN and other international organizations, particularly the IAEA, but not exclusively. For it to succeed, it is essential to ensure that each country takes the appropriate nuclear security measures; in this spirit the Communiqué lists a number of voluntary actions that States can take in order to give the international community assurances on the effectiveness of the implementation of nuclear security measures at the national level.

National commitments and Gift Baskets

The Communiqués and the Washington Work Plan are the only deliverable of the Nuclear Security Summits. However, since the Washington Summit there have been additional commitments which initially were essentially unilateral, known as "house gifts".
Seoul saw the introduction of the concept of "Gift Baskets", which are multinational joint statements. Their role was refined in the two years leading up to the The Hague Summit and they are now seen as an

I risultati

I risultati del processo NSS sono sia politici che pratici. Facendo riferimento ai passi concreti avviati a livello nazionale e internazionale, molti esempi sono stati presentati in occasione della IAEA Nuclear Security Conference di luglio 2013. Al Summit de L'Aja, lo stesso Presidente Obama ha citato i principali risultati, come riportato nel Riquadro 2.

La dimensione della minaccia

Uno dei primi obiettivi del processo NSS era accrescere la consapevolezza del fatto che la minaccia nucleare è una realtà concreta. Lo scenario di un attacco terroristico nucleare è stato preso seriamente in considerazione solo a partire dall'11 Settembre.

Sebbene non esistano prove che terroristi siano in grado di fabbricare un'arma nucleare, si pensa che ordigni nucleari improvvisati (IND - Improvised Nuclear Device) o altri ordigni in grado di disperdere radioattività (RDD - Radiological Dispersal Device, anche conosciuti come "dirty bomb" e "bomba sporca"), possano essere alla portata delle capacità tecniche dei terroristi. Anche se gli effetti di un ordigno nucleare (i.e. con reazione a catena), seppur improvvisato, sarebbero di un ordine di grandezza superiore a quelli di una "bomba sporca", molti considerano che quest'ultimo scenario rappresenti la minaccia principale a causa della relativa semplicità di progettazione e della maggiore disponibilità di materiale radioattivo. Il sabotaggio di impianti contenenti materiale nucleare e altro materiale radioattivo è un ulteriore, possibile, scenario.

La protezione del materiale nucleare e altro materiale radioattivo e degli impianti associati è il primo e più importante passo per prevenire un evento di security nucleare ed è il focus dei tre Communiqué e del Work Plan di Washington.

La protezione di armi nucleari, che implica uno scenario di furto da strutture militari, è stata trattata solo marginalmente nei Summit.

Materiale nucleare

I materiali nucleari di interesse per il processo NSS sono l'HEU e il plutonio, ovvero materiali che, anche quando non di qualità militare (weapon-grade [6]), sono direttamente utilizzabili per un ordigno nucleare senza dover ricorrere a ulteriori tecnologie di arricchimento o di riprocessamento, che sono considerate al di là della portata dei terroristi (almeno per ora). La quan-

important contribution to further strengthening the Communiqué.

At The Hague, Italy presented a Gift Basket on *"Nuclear Security Training and Support Centres / Centres of Excellence (NSSC/CoE)"* [5] which aims to demonstrate the progress achieved since the Washington Summit, while further promoting the development of nuclear security training and support centres/centres of excellence, and deepening international and regional cooperation. This Gift Basket and its success may be seen as a recognition of Italy's efforts in the NSS process to strengthen the nuclear security culture. At the Washington Summit, which gave unprecedented importance to the human dimension, Italy made a national commitment for the establishment, together with the IAEA and the International Centre for Theoretical Physics (ICTP), of an International Nuclear Security School in Trieste: the School held its first course one year later in April 2011, and the fourth course was held in 2014.

The achievements

The achievements of the NSS process are both at the political and practical levels. With respect to the concrete steps taken nationally and internationally to strengthen nuclear security, many examples were shown at the IAEA Nuclear Security Conference in July 2013. In The Hague, President Obama himself made a list of the principal achievements, as shown in Box 2.

The threat dimension

One of the first goals of the NSS process was to broaden the understanding that the nuclear threat was real. The scenario of a nuclear terrorist attack has been taken seriously into account since 9/11. Although there is no evidence that terrorists could manufacture a nuclear weapon, there is a belief that an Improvised Nuclear Device (IND) or other devices for spreading radioactivity, such as a Radiological Dispersal Device (RDD) might be within reach of the technical capability of terrorists. Although the effects of a nuclear device (i.e. with a chain reaction) would be one order of magnitude greater than those of a device dispersing radioactivity, many consider that the major threat is to be found in the latter scenario, because of the relative simplicity of the design and greater availability of radioactive material. The sabotage of facilities containing nuclear and other radioactive material is another possible scenario.

The protection of nuclear and other radioactive material and associated facilities is the first and most important step to prevent a nuclear security event and is the focus of the Communiqués and the *tità di HEU e di plutonio presente nel mondo è motivo di grande preoccupazione, in particolare se confrontata con le quantità necessarie per fabbricare un ordigno nucleare: anche un ordigno grezzo non richiede più di qualche decina di Kg di HEU e meno di 10 Kg di plutonio. La Tabella 2 riporta le quantità (stimate) di HEU e di plutonio presenti in diversi Paesi, ripartite tra scopi civili e militari. In tutto il mondo esistono circa 1400 tonnellate di HEU (con un ampio margine di incertezza) e 500 tonnellate di plutonio separato, 260 delle quali destinate ad uso civile [7].*

Negli anni molti sforzi e risorse sono stati dedicati dalla comunità internazionale alla messa in sicurezza di questi materiali, particolarmente a seguito del collasso dell'Unione Sovietica, quando furono scoperti i primi casi di traffico illecito di materiale nucleare. Ma resta ancora molto da fare. La messa in sicurezza del HEU e plutonio nell'arco di quattro anni è l'obiettivo del NSS, evidentemente più un'aspirazione che una previsione realistica. Tuttavia, in molti Paesi il processo NSS ha accelerato l'applicazione di misure per la protezione fisica di materiali e impianti che altrimenti avrebbero richiesto anni; oppure in molti Paesi, come nel caso dell'Italia, ha portato al rimpatrio di HEU e plutonio nei Paesi di origine.

Diversi impegni a livello nazionale e Gift Basket supportano ulteriormente il Communiqué in questo sforzo. Il rimpatrio dall'Italia, a seguito dell'impegno preso a Seoul, è stato molto apprezzato durante il Summit de L'Aja (vedi anche Riquadro 2).

Materiali radioattivi

La preoccupazione per la security delle sorgenti radioattive e, più in generale, dei materiali radioattivi (oltre a HEU e plutonio) e delle strutture ad essi associate, è andata crescendo negli ultimi anni ed è ora considerata da molti analisti la vera priorità a causa della relativa vulnerabilità delle sorgenti radioattive rispetto al materiale nucleare.

Sebbene gli effetti non siano paragonabili a quelli dell'esplosione di un ordigno nucleare, anche grezzo, e non vi sia notizia di attacchi, l'AIEA ha documentato parecchi incidenti legati a materiale radioattivo con gravi conseguenze. Quello più noto e generalmente utilizzato come caso di riferimento è l'incidente di Goiania (Riquadro 3), che dimostra come le conseguenze per la società siano a vari livelli [8].

Anche la dimensione della minaccia è di proporzioni enormi:

Achievements of the Nuclear Security Summit Process

In previous summits, as a consequence to the work that's been done collectively:

- 12 countries and two dozen nuclear facilities around the world have rid themselves entirely of HEU and plutonium.
- Dozens of nations have:
  - boosted security at their nuclear storage sites;
  - built their own counter-smuggling teams;
  - or created new centers to improve nuclear security and training.
- The IAEA is stronger.
- More countries have ratified the treaties and international partnerships at the heart of our efforts.

At this particular summit,

- Belgium and Italy completed the removal of their excess supplies of HEU and plutonium so that those supplied can be eliminated.
- In a major commitment, Japan announced that it will work with the United States to eliminate hundreds of kilograms of weapons-usable nuclear material from one of their experimental reactors, which would be enough for a dozen nuclear weapons.
- Dozens of other nations have agreed to take specific steps towards improving nuclear security in their own countries and to support global efforts.

BOX 2 The NSS process achievements. Excerpt from President Obama's remarks at the Closing session of the NSS in The Hague

Risultati del processo NSS. Estratto dalla dichiarazione del Presidente Obama durante la sessione conclusiva del Summit de L'Aja

Source: The White House, Office of the Press Secretary

Washington Work Plan. The protection of nuclear weapons, which implies a scenario of theft from military facilities, is addressed only marginally by the Summits.

Nuclear material

The nuclear material of interest for the NSS process is HEU and plutonium, i.e. material not necessarily weapons-grade [6] but directly usable for a nuclear device without further processing - enrichment or reprocessing – technologies considered beyond the reach of terrorists (at present). The amount of HEU and plutonium around the world is cause for grave concern, particularly in relation to the quantities needed for a nuclear device: even a crude device does not require more than a few dozen kg of HEU and less than 10 kg of plutonium. Table 2 shows the estimated amount of HEU and plutonium (distinguishing between

	HEU	Non-civilian Pu	Civilian Pu
Russia	695	128	50.1
United States	604	87.0	0
France	31	6	57.5
China	16	1.8	0.014
United Kingdom	21.2	3.5	91.2
Pakistan	3	0.15	0
India	0.8	5.2	0.24
Israel	0.3	0.84	-
North Korea	0	0.03	-
Others	15	-	61
TOTAL	**1,390**	**234**	**260**

TABLE 2 Estimated quantities of HEU and plutonium (tonnes) as of January 2013
Stima delle quantità di HEU e plutonio separato (tonnellate) a gennaio 2013
Source: International Panel on Fissile Materials, http://www.fissilematerials.org

- *milioni di sorgenti radioattive sono largamente usate in medicina, industria, agricoltura, ricerca, ecc., (anche se solo una frazione può essere una seria minaccia per la security);*
- *le sorgenti radioattive sono diffuse in tutto il mondo, mentre i produttori risiedono solo in pochi Paesi: l'AIEA stima che vi siano migliaia di operazioni di trasporto al giorno (su strada, ferrovia, per via aerea o per mare);*
- *migliaia (stima) di sorgenti orfane, cioè fuori dal controllo normativo, sono ancora in circolazione, inoltre si tratta spesso di sorgenti non convenzionali, come i generatori termoelettrici a radioisotopi (RTG - radioisotope thermoelectric generator);*
- *anche le sorgenti sotto controllo spesso non sono adeguatamente messe in sicurezza, ad esempio si trovano in aree non protette e con protezione fisica limitata e/o libero accesso, come gli ospedali.*

Particolarmente preoccupanti sono le sorgenti a fine vita perché, in assenza di una strategia di gestione nazionale a lungo termine che copra la sorgente lungo tutto il suo arco di vita (from "the cradle to the grave"), corrono il rischio di essere abbandonate e di diventare sorgenti orfane. La mancanza di depositi nazionali, nonché i costi e i problemi legati al trasporto, aumentano la preoccupazione. Le sorgenti trafugate, abbandonate ed eventualmente orfane (Fig. 3) potrebbero essere trasportate facilmente e potenzialmente utilizzate per scopi malevoli.

civilian and military purposes) in several countries. Worldwide there are around 1,400 tonnes of HEU (with a wide margin of uncertainty) and 500 tonnes of separated plutonium, 260 of which are for civilian use [7].

Many efforts and resources have been dedicated by the international community to securing this material over the years, particularly after the collapse of the Soviet Union, when the first cases of illicit trafficking of nuclear material were discovered, but still much needs to be done. Securing the HEU and plutonium in the space of four years is the goal of the NSS, evidently more of an aspirational goal than a realistic one. Nevertheless, in many countries this has accelerated the implementation of security measures for the physical protection of nuclear material and associated facilities that otherwise could have taken years; or, in several countries, as in the case of Italy, has brought to the repatriation of HEU and plutonium to the countries of origin.

Several national commitments and Gift Baskets further support the Communiqué in this effort. The repatriation from Italy, following the Italian commitment taken in Seoul, was highly commended during the Summit in The Hague (see also Box 2).

Radioactive material

Concern for the security of radioactive sources and more in general radioactive material (other than HEU and plutonium) and associated facilities has been steadily growing in recent years. Many analysts see it as the key priority because of the relative vulnerability of radioactive sources with respect to nuclear material.

The Goiania Case

In 1985, a Cs-137 teletherapy unit was left in an abandoned clinic without notification to the Safety Authorities. Two years later, scrap scavengers stole the unit and, after dismantlement, sold it to a junkyard: the source capsule was then broken and 50.9 TBq of Cs-137 in the form of CsCl powder were released and spread in the Goiania urban environment.

L'incidente di Goiania

Nel 1985, una unità di teleterapia che utilizzava Cs-137 fu abbandonata in una clinica dismessa senza che ne fosse informata l'Autorità di Sicurezza. Due anni dopo, l'unità fu rubata da cercatori di rottami e, una volta fatta a pezzi, venduta a un rottamaio. La capsula con la sorgente finì in una discarica dove fu aperta rilasciando 50.9 TBq di Cs-137 sotto forma di polvere di CsCl che si diffusero nell'area urbana di Goiania.)

Goiania (Brazil), 1987, impact on Goiania City:

- 360 persons contaminated including 124 with internal and/or external contamination
- 4 persons died within four weeks
- About 125,000 persons monitored (10% population) until February 1988 over an area of 67 km^2
- 4 hospitals, 42 residences, numerous public buses and private cars heavily contaminated
- Over 3,500 m^3 of accumulated radioactive waste

Cost: > 20 M USD

Goiania (Brazil), 1987, effects on the population:

- Airline pilots refuses to fly aircraft with Goiania residents on board
- Drivers refused to allow Goiania residents to board their buses
- Cars with Goiania license plates were stoned outside the city limits
- Hotels in Sao Paulo and other cities did not let Goiania residents check in
- Over 8,000 residents requested and received official certificates of "uncontaminated persons"
- Demand for locally-produced industrial and agricultural products dramatically dropped nationwide leading to numerous bankruptcies and high unemployment

BOX 3 Consequences of the radiological accident in Goiania, Brazil
Conseguenze dell'incidente radiologico di Goiania (Brasile)
Source: IAEA

Although the effects are not comparable to the explosion of a nuclear device, even a crude one, and there are no known cases of attacks, the IAEA has documented several incidents involving radioactivity with serious consequences. The most widely known and generally used as a benchmark is the Goiania case (Box 3) which shows that the consequences for society are at several levels [8].

Non sorprende, quindi, che il processo NSS stia prestando maggiore attenzione alla security dei materiali radioattivi. Oltre agli impegni espressi nei Communiqué, al Summit de L'Aja è stato lanciato dagli Stati Uniti un nuovo Gift Basket con l'obiettivo di intensificare la security radiologica: finora 35 Paesi, tra cui l'Italia,

Inadequate Source Stores

Eventually, sources became *unneeded* and *disused*; where no disposal path exists, they are often simply *abandoned!*

IAEA

7

FIGURE 3 Example of inadequate source store

Esempi di depositi inadeguati per le sorgenti

Source: IAEA, International Conference on the Safety and Security of Radioactive Sources, Abu Dhabi, Oct 2014

The threat dimension is also huge:

- millions of radioactive sources are widely used in medicine, industry, agriculture, research, etc. (but only a fraction give rise to serious security concerns);
- radioactive sources are widespread around the world, though producers are located only in a few countries: the IAEA estimates that there are thousands of transport operations daily (by road, rail, air and sea);
- thousands (estimated) orphan sources, i.e. out of regulatory control, are still in circulation and are often non-conventional sources, such as Radioisotope Thermoelectric Generators;
- often also the regulated sources are not properly secured, e.g. in non-protected areas and with limited physical protection and/or open access, such as hospitals.

Of particular concern are the sources at the end of their life because, in the absence of a long-term national management strategy covering the source from “the cradle to the grave”, they run the risk of being abandoned and becoming orphan sources. There is particular concern over the lack of national repositories, and with regard to the costs and problems of transportation. The diverted, abandoned and orphaned sources (Fig. 3) could be effortlessly transported and potentially used for malevolent purposes.

As a result it is not surprising that the NSS process has been paying greater attention to the security of radioactive materials. In addition to the Communiqué commitments, in The Hague a new Gift Basket was launched by the US for strengthening radiological security. So far 35 countries, including Italy, have committed themselves to securing all Cat.1 sources by 2016 and to transposing the relevant international instruments into the national legislation.

Illicit trafficking

The Incident and Trafficking Database (ITDB) of the IAEA from its institution in 1995 until December 2012 recorded 2331 accidents involving nuclear and other radioactive material: of these 419 were of a criminal nature and 16 involved HEU or plutonium [9]. Although at

si sono impegnati a mettere in sicurezza tutte le sorgenti di Cat.1 entro il 2016 e a trasporre i pertinenti strumenti internazionali nelle legislazioni nazionali.

Traffico illecito

L’Incident and Trafficking Database (ITDB) dell’AIEA, dalla sua istituzione nel 1995 fino a dicembre 2012, ha registrato 2331 casi, principalmente ritrovamenti, associati a materiale nucleare e altro materiale radioattivo: di questi, 419 erano di natura criminale e 16 riguardavano HEU o plutonio [9]. Sebbene a livelli diversi dagli anni Novanta, i recenti ritrovamenti continuano a confermare l’esistenza di materiale non adeguatamente protetto e di individui o gruppi pronti a approfittarne per traffici illeciti.

Il processo del Nuclear Security Summit riconosce pienamente la dimensione internazionale della lotta al traffico illecito. Cooperazione e condivisione delle informazioni su scala internazionale sono fattori chiave di questa lotta, insieme allo sviluppo e scambio di conoscenze *e tecniche per il forense nucleare. Quest'ultima disciplina è molto importante per individuare l'origine del materiale nucleare e altri materiali radioattivi e per raccogliere prove da utilizzare nei processi contro il traffico illecito dei materiali e il loro uso a fini criminali.*

Alcuni Gift Basket e impegni nazionali supportano ulteriormente i Communiqué. L'Italia ha assunto un impegno specifico al Summit di Washington relativo alla Megaport Initative, un'iniziativa statunitense intesa a prevenire il contrabbando di materiale nucleare e altro materiale radioattivo tramite un sistema marittimo globale. Secondo il Progress Report nazionale presentato dall'Italia [10] al NSS-2014: "Since September 2013 the ports of Genoa and La Spezia have been equipped with mobile detection systems. By the end of December 2013 more than 300 cargo shipments have been controlled."

Il quadro internazionale

L'AIEA e altri forum internazionali

Sebbene la security non sia specificatamente menzionata nel suo statuto, l'AIEA svolge un ruolo chiave nel coordinamento degli sforzi internazionali per rafforzare l'architettura globale per la security nucleare, così come riconosciuto anche dal Communiqué rilasciato a L'Aja: "35. Our representatives will therefore continue to participate in different international forums dealing with nuclear security, with the IAEA playing the leading role in their coordination".

Tutti i Communiqué hanno sostenuto le attività dell'AIEA in supporto agli Stati Membri: dai documenti della Nuclear Security Series, ai servizi di Peer Review e Advisory, in particolare l'International Physical Protection Advisory Service (IPPAS), e alle attività per lo sviluppo di competenze. Per queste ultime, l'AIEA offre un esteso programma di training a livello nazionale e regionale e ha creato due network internazionali: l'International Nuclear Security Education Network (INSEN) per le università e l'International Network for Nuclear Security Training and Support Centres (NSSC Network) per i centri di training e supporto.

Il segmento Ministeriale dell'International Conference on Nuclear Security di luglio 2013, con 1300 partecipanti provenienti da 125 Stati Membri, 34 dei quali rappresentati a livello ministeriale, ha mostrato la capacità dell'AIEA di saper trattare con successo problematiche politiche, strategiche, tecniche e normative in un singolo evento e di poter portare la consapevolezza sulla security nucleare ad un livello go-

different levels than in the 1990s, recent findings continue to confirm the existence of nuclear and other radioactive material that is not adequately secured and of individuals or groups ready to illicitly traffic such material.

The Nuclear Security Summit process fully recognizes the international dimension of the campaign against illicit trafficking. International cooperation and information-sharing are the key factors in this campaign, together with the development and sharing of nuclear forensic capabilities for determining the origin of nuclear and other radioactive materials and for providing evidence to be used in the prosecution of acts of illicit trafficking and malicious uses.

A number of Gift Baskets and national commitments further support the Communiqué. Italy made a specific commitment at the Washington Summit on the Megaport Initative, a US initiative intended to prevent the smuggling of nuclear and other radioactive materials through the global maritime system. According to the Italian National Progress Report [10] to the NSS-2014: *"Since September 2013 the ports of Genoa and La Spezia have been equipped with mobile detection systems. By the end of December 2013 more than 300 cargo shipments have been controlled."*

The international framework

The IAEA and other international fora

Although security is not specifically mentioned in its statute, the IAEA is now playing a key role in coordinating international efforts to strengthen the global nuclear security architecture, as also recognized by the Communiqué issued in The Hague: "35. *Our representatives will therefore continue to participate in different international forums dealing with nuclear security, with the IAEA playing the leading role in their coordination".*

All Communiqués have sustained the IAEA activities in support of Member States: from the drafting of the documents of the Nuclear Security Series, the Peer Review Missions and Advisory Services, in particular the International Physical Protection Advisory Service (IPPAS), and capacity-building activities. These activities include the extensive training course programmes at the national and regional levels, and the creation of the International Nuclear Security Education Network (INSEN) and of the International Network for Nuclear Security Training and Support Centres (known as the NSSC Network).

The Ministerial session of the International Conference on Nuclear Security in July 2013, with 1300 participants from 125 Member States, 34 represented at Ministerial Level, showed the IAEA's capacity to successfully address political, policy, technical and regulatory issues in one single event and to raise global awareness on nuclear security *bale. La convocazione di Conferenze Ministeriali AIEA su base periodica è una delle opzioni prese in esame per il futuro del processo NSS.*

Gli altri forum internazionali relativi alla security nucleare citati dai Communiqué sono le Nazioni Unite, l'Iniziativa globale per la lotta contro il terrorismo nucleare (Global Initiative to Combat Nuclear Terrorism) e la Global Partnership.

Le Nazioni Unite hanno contribuito in modo significativo al rafforzamento del quadro globale della security nucleare, in particolare mediante la Risoluzione 1540 del Consiglio di Sicurezza delle Nazioni Unite. Adottata nel 2004, la Risoluzione impone a tutti gli Stati, inter alia, l'obbligo di adottare e applicare una legislazione nazionale contro la proliferazione di armi nucleari, chimiche e biologiche e dei relativi vettori, e di stabilire adeguati controlli interni sui materiali per prevenirne il traffico illecito. Un Gift Basket sponsorizzato dal Canada e dalla Corea del Sud, che riconferma l'impegno a rispettare gli obblighi per migliorare la security dei materiali nucleari nel mondo, ha raccolto ampio consenso tra i Paesi del NSS.

La Global Initiative to Combat Nuclear Terrorism (GICNT) ha condotto un grande numero di attività multilaterali significative ai fini del processo NSS, con l'obiettivo di ottenere risultati tangibili quali, ad esempio, la condivisione di buone pratiche e delle lesson learned su pianificazione, strategie, procedure e interoperabilità.

La Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP) è un partneriato istituito nel 2002 durante il Summit G8 di Kananaskis (Canada) con il focus sulla Russia e con lo scopo di prevenire l'acquisizione di armi di distruzione di massa da parte di terroristi. Al Summit G8 di Deauville (Francia), la Global Partnership è stata estesa oltre il 2012, data originariamente prevista per il suo completamento, e la sua partecipazione è stata allargata anche a Paesi non appartenenti al G8.

Gli strumenti internazionali

L'incoraggiamento ad attenersi agli strumenti esistenti e la riduzione del divario nella attuazione nazionale è uno degli obiettivi del processo NSS: è infatti evidente che un regime globale di security nucleare non può essere robusto ed efficace fino a che tutti i Paesi non abbiano messo in atto un regime nazionale di security nucleare.

Anche gli strumenti legislativi presentano punti deboli. Per il materiale nucleare, il gap più rilevante è la mancata entrata in vigore dell'emendamento del 2005 alla Convenzione sulla protezione fisica del materiale nucleare (CPPNM)

issues. The holding of IAEA Ministerial Conferences on a periodical basis is one of the options under examination for the future of the NSS process.

The other international fora relevant to nuclear security, as per the Communiqués, are the UN, the Global Initiative to Combat Nuclear Terrorism, and the G8 Global Partnership.

The United Nations has made a significant contribution to the strengthening of the global nuclear security framework, in particular with the UN Security Council Resolution 1540. This Resolution, dated 2004, imposes on all States, inter alia, an obligation to implement national legislation to prevent the proliferation of nuclear, chemical and biological weapons and their means of delivery, and to establish appropriate domestic controls over relevant material to prevent their illicit trafficking. A Gift Basket sponsored by Canada and South Korea, reaffirming the commitment to implement the obligations to enhance the security of nuclear materials worldwide, gained widespread consensus among the NSS countries.

The Global Initiative to Combat Nuclear Terrorism (GICNT) has conducted a large number of multilateral activities relevant to the objectives of the NSS process. They have been focusing on the delivery of tangible results, such as the sharing of best practices and lesson learned on plans, policies, procedures, and interoperability.

The Global Partnership (GP) Against the Spread of Weapons and Materials of Mass Destruction (WMD) was launched at the G8 Summit of Kananaskis, Canada, in 2002, with the specific focus on Russia and the aim of preventing terrorists from acquiring weapons of mass destruction. At the Deauville G8 Summit, the Global Partnership was extended beyond 2012, the date originally foreseen for its completion, and membership was extended to non-G8 countries.

The international instruments

The promotion of adherence to the existing instruments and the reduction of the gaps in national implementation is one of the aims of the NSS process: clearly, a global nuclear security regime cannot be strong and effective until all countries have implemented a national nuclear security regime.

The legal instruments also present gaps. The most relevant ones, with regard to nuclear material, are the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) and, for radioactive sources, the lack of legally binding instruments. In this case, the most relevant one is the Code of Conduct on the Safety and Security of Radioactive Sources, together with the Supplementary Guidance on the Import and Export of Radioactive Sources, which has a widespread consensus but is not legally binding.

e, per quanto riguarda le sorgenti radioattive, la mancanza di strumenti legalmente vincolanti. In questo caso, lo strumento principale è il Codice di Condotta sulla Safety e la Security delle Sorgenti Radioattive, che ha riscosso ampio consenso ma è, appunto, privo di vincoli legali.

Conclusioni

Prima dell'annuncio del Presidente Obama a giugno 2013 che gli Stati Uniti avrebbero ospitato un Nuclear Security Summit nel 2016, molti ritenevano che quello de L'Aja sarebbe stato l'ultimo, concludendo il ciclo con la consegna del processo all'AIEA a Vienna. Anche se non è stato così, il Summit de L'Aja può comunque essere considerato un punto di svolta per il processo NSS.
Nel suo discorso conclusivo, il Presidente Obama ha dichiarato che il prossimo sarà un Summit di transizione: come e dove porterà, sarà deciso dai leader che vi prenderanno parte. Tuttavia le basi per questa decisione saranno gettate nei prossimi due anni a livello di Sherpa nel circuito del Nuclear Security Summit.

(traduzione di Carla Costigliola)

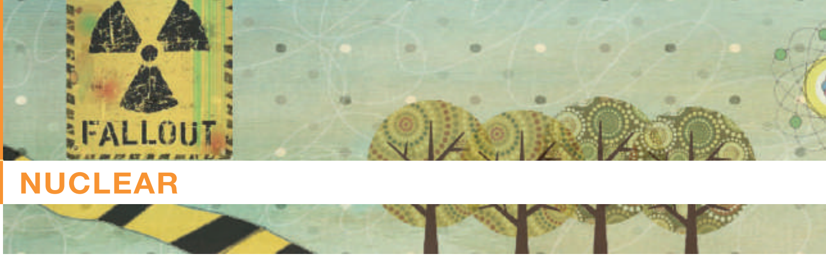
Conclusions

Before President Obama's announcement in June 2013 that the US would host a Nuclear Security Summit in 2016, many believed that the Nuclear Security Summit in The Hague was to be the last one, concluding the cycle with the handing over of the process to the International Atomic Energy Agency (IAEA) in Vienna.
Although this was not the case, the Summit in The Hague can still be considered to be a turning point for the NSS process. In his concluding speech in The Hague, President Obama declared that next one would be a transition Summit: how and where it will go will be decided by the leaders taking part, but in the two intervening years the groundwork for this decision is to be laid at Sherpa level in the Nuclear Security Summit circuit.

Franca Padoani
ENEA, Technical Unit for Reactor Safety and Fuel Cycle Methods -
Reactor Core and Shielding Analysis and Design Laboratory

references & notes

[1] 2010, Communiqué of the Washington Nuclear Security Summit (https://www.nss2014.com/sites/default/files/documents/11.communique.pdf).
[2] 2010, Work Plan of the Washington Nuclear Security Summit (https://www.nss2014.com/sites/default/files/documents/12.work_plan.pdf).
[3] 2012, Seoul Communiqué - 2012 Seoul Nuclear Security Summit (https://www.nss2014.com/sites/default/files/documents/seoul_communique_final.pdf).
[4] 2014, The Hague Nuclear Security Summit Communiqué (https://www.nss2014.com/sites/default/files/documents/the_hague_nuclear_security_summit_communique_final.pdf).
[5] 2014, "Joint statement on Nuclear Security Training and Support Centres/ Centres of Excellence" (https://www.nss2014.com/sites/default/files/documents/joint_statement_nssc-coefinal_24_march_2014.pdf).
[6] Uranium weapons-grade: U-235>85%. For plutonium, the amount of Pu-240 defines the grade: Super-grade < 3%, Weapons-grade < 7%, Fuel-grade 7-18%, Reactor-grade >18%. The higher the content of Pu-240, the greater the difficulty of manufacturing a nuclear device.
[7] International Panel on Fissile Materials, 2013, Fissile material stocks (http://www.fissilematerials.org).
[8] International Atomic Energy Agency Vienna, 1988, The radiological accident in Goiania (http://www-pub.iaea.org/mtcd/publications/pdf/pub815_web.pdf).
[9] International Atomic Energy Agency Vienna, 2014, IAEA Incident and Trafficking Database (ITDB) Incidents of nuclear and other radioactive material out of regulatory control - 2014 Fact Sheet (http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf).
[10] 2014, Nuclear Security Summit 2014 - National Progress Report Italy (https://www.nss2014.com/sites/default/files/documents/italy.pdf).ì



Progetto europeo EDEN: la Thematic Demo sull'ispezione 3D laser in un reattore nucleare

Il progetto europeo EDEN rappresenta uno sforzo senza precedenti, da parte della Commissione Europea, a supporto delle attività di Ricerca e Sviluppo nel settore CBRNe. Sulla base dei risultati e delle lezioni apprese in precedenti progetti nazionali e internazionali, EDEN ha l'obiettivo di portare a un livello superiore di integrazione strumenti e pratiche atti a prevenire e ad affrontare situazioni di emergenza. Le soluzioni ricercate saranno validate sul campo tramite esercizi di simulazione di situazioni il più possibile simili alle condizioni reali. L'ENEA è attualmente impegnata in uno di questi esercizi dimostrativi, indicati nel progetto come Thematic Demos, dedicato alla realizzazione di uno scanner 3D per ispezioni avanzate negli ambienti acquosi di un impianto nucleare (serbatoio e vasca di stoccaggio). Il presente contributo definisce le linee guida di questa azione, programmata per il prossimo Settembre 2015, che pone l'ENEA all'avanguardia nella ricerca sui metodi innovativi di ispezione per l'industria nucleare. Viene inoltre fornita una breve descrizione del concetto e della struttura del progetto europeo EDEN, al fine di contestualizzare meglio l'azione descritta.

The European EDEN project: Thematic Demo on 3D laser inspection in a nuclear reactor

The European EDEN project marks an unprecedented effort of the European Commission to support Research & Development actions in the field of CBRNe. Building upon the results and lessons learnt in previous national and international projects, EDEN aims at bringing to a next level of integration tools and practices for preventing and facing emergency situations. The solutions sought will be validated through in-field exercises with simulated situations resembling real conditions as far as possible. ENEA is leading one of these exercises, indicated in the project as Thematic Demos and devoted to the realization of a 3D laser scanner for improved inspection in the wet environments of a nuclear facility (nuclear vessel and storage pool). The present contribution outlines the guidelines of this action scheduled for September 2015, which puts ENEA at the forefront of the research in the field of innovative inspection methods for nuclear industry. A short description of the EDEN project concept and structure is given for better framing the action.

DOI: 10.12910/EAI2014-96

■ *L. De Dominicis, A. Palucci, M. Carta, M. Ferri de Collibus, R. Fantoni, G. Fornetti, M. Francucci, M. Guarneri, M. Nuvoli, M. Palomba, E. Santoro, M. Sepielli*

■ **Contact person: Luigi De Dominicis**
luigi.dedominicis@enea.it

The EDEN project as a whole

The accidental or deliberate release of CBRNe materials are low probability events that can have a significant impact on citizens and society. Whenever and wherever they occur, they usually require a gradual and multifaceted response as they tend to provoke severe and unexpected physical, psychological, societal, economic and political effects that might also easily cross the borders inside and outside the EU.

Research activities are essential to develop new instruments and tools that the end-users can activate for successfully managing the four phases of the emergency management, which include Mitigation, Preparedness, Response, and Recovery.

The European Commission has strongly backed the efforts that the private and public sectors are carrying on to secure Europe a leading position as provider of hardware, methodologies and practice for handling emergency situations.

Within the Seventh Framework Programme (FP7), which covered the 2007-2013 period, the European Commission has sustained the theme Security, and CBRNe in particular, as a pillar of its institutional action to promote the European development through research. Many of the main projects are still under completion and at their final stage. Among them, PRACTICE (Preparedness and Resilience Against CBRNe terrorism Using Integrated Concepts and Equipment [1]) and DECOTESSC1 (DECOTESSC1 - Demonstration of Counter Terrorism System-of-Systems against CBRNe phase 1 [2]) are worth mentioning as they mark a considerable progress with respect to the default situation, characterized by a fragmented structure in terms of technology, procedures, methods and organization at the national and EU levels.

As a final act of the FP7 the European Commission has funded an integrated project, EDEN (End-user driven Demo for CBRNe), with an unprecedented economic effort.

The EDEN project [3] will leverage the added-value of tools and systems from previous R&D efforts and improve CBRNe resilience through their adaptation and integration in complex multinational/agency CBRNe operations. The EDEN project stems from the clear understanding that successful CBRNe resilience requires a global System-of-Systems approach.

EDEN recognises that "Systems of systems" has a different meaning for different countries and protection agencies and the concept of the EDEN project is to provide a "toolbox of toolboxes" (ToT), from a virtual EDEN Store, to allow different stakeholders to have a common certified set of applications available and pick the capabilities they deem important (or affordable) from them.

This concept will allow a high degree of interoperability at the differing levels of capability that each country may have. The benefit of EDEN concept is that integration is immediately applied at the application level.

The EDEN Store concept allows capabilities to be shared and consistently provided and accessible to multiple stakeholders. It will gradually build up a common capability that will span across the European boundaries. It will also share the burden of development and allow for lessons to be learned and applications to be enhanced based on the learning. Most importantly, it provides for interoperability, which is paramount in cross-boundary incident management.

Validation will be through three themed end-user demonstrations (Food Industry, Multi-Chemical, Radiological) cover at multiple hazards (C, B, R, N, E), and multiple phases of the security cycle, multiple tiers of and multiple stakeholders.

The EDEN consortium includes end-users, major stakeholders in the CBRNe domain, and large system integration and system solution providers, including SMEs (Small and Medium-sized Enterprises) that will bring innovative solutions and support integration and RTOs (Research and Technology Organisations) that will further develop EU affordable resilience.

The expected impact from EDEN is to provide affordable CBRNe resilience and market sustainability through the better system integration in real operations and in enhancing the safety of citizens.

The concept behind the EDEN Store is summarized in Figure 1.

End-User needs, as identified with a survey carried out prior to the project start and steadily updated during the project execution, are the main drivers of EDEN. They are the input for the development of the

"Toolbox of Toolboxes", which will include both new and existing tools coming from previous projects.
With a consortium of 39 partners, EDEN gathers most of the principal stakeholders together in R&D activities on CBRNe. The project has a three-year expected duration and the kick-off was on September 1st, 2013. The focal points of the whole project will be three large-scale demonstration actions scheduled at the end of the project, during which the ToT will tested and validated.
The three Demo actions are broken down into:

- Food chain and biological contamination
- Multi-chemical threat
- Radiological threat

Besides them, Thematic Demos include a plurality of scheduled actions, during which specific tools and practices will be tested and validated through in-field exercise. One of these Thematic Demos is led by ENEA and is about the development of a 3D laser scanner for inspection in the wet environments of a nuclear reactor. Wet environments include the vessel containing the core of the reactor and the storage pool for spent fuel rods. To complete this ambitious task ENEA will build upon its proven track record in developing 3D laser scanners for terrestrial and underwater applications. Here the challenge is to develop a device qualified for operating in a contaminated environment, a target that demands specific scientific and technological solutions. Inspections in nuclear reactors are essential for preventing faults, planning repairs and replacing critical components. Although laser techniques for measuring quantitatively fuel rods deformation have already attracted the interest of some research groups [4], so far tests have only been carried out in laboratory. The action ENEA is leading within EDEN aims at deploying for the first time a 3D laser sensor

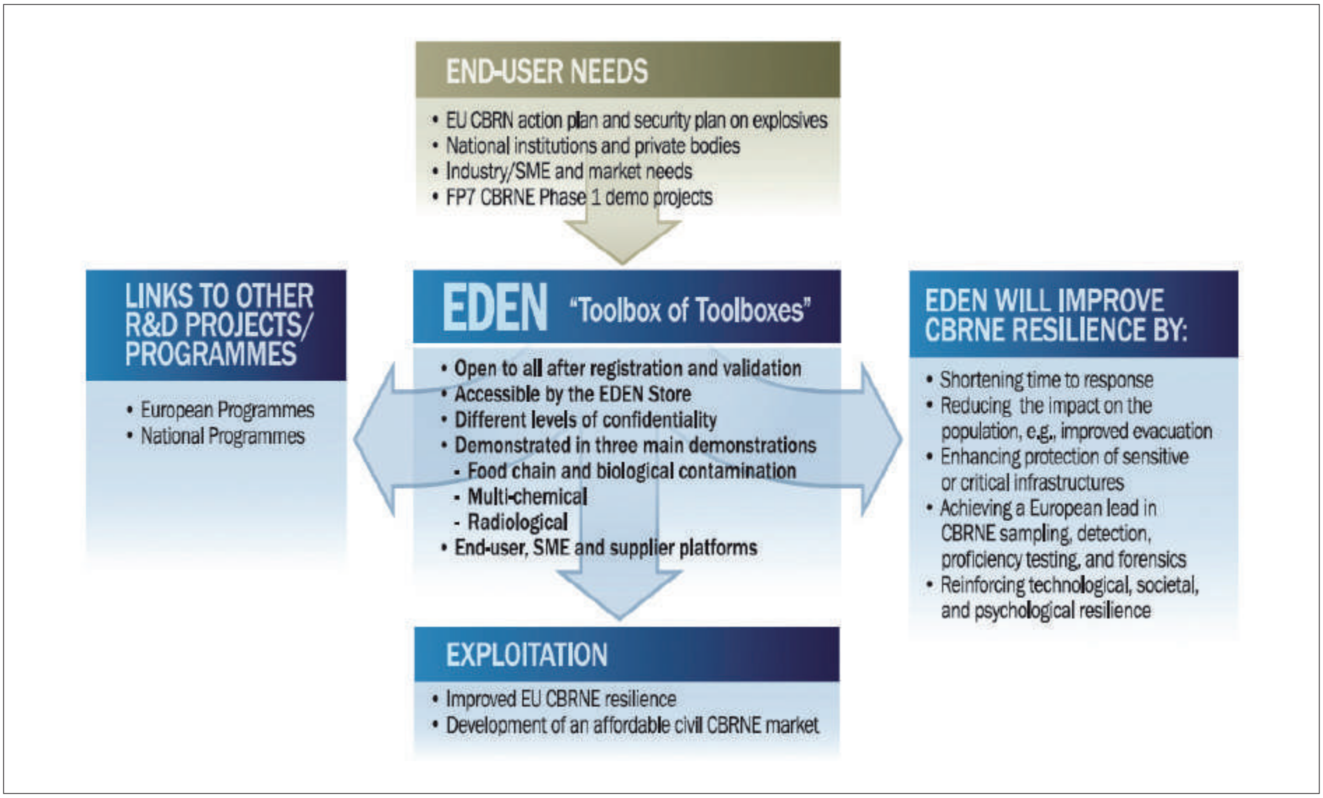


FIGURE 1 The EDEN project concept summarized in a workflow

in the wet and contaminated environment of a nuclear reactor, paving the way for further technological developments in this research field.

Thematic Demo on improved inspection in a nuclear reactor using 3D laser scanning technique

This action is about the demonstration of a new 3D laser scanner for the surveillance of the deterioration condition of nuclear fuel rods. The device will be immersed inside the storage pool and/or in the reactor pool for inspecting the fuel rods remotely.

Despite the numerous existing typologies of nuclear reactors (Boiling Water Reactors, Pressurized Water Reactors, TRIGA research reactors, etc.), the common physical forms of nuclear fuel is cylindrical, with the fuel pellets inserted into metallic tubes.

Cladding is the outer layer of fuel rods, standing between the coolant and the nuclear fuel. It is made of a corrosion-resistant material with low absorption cross-section for thermal neutrons, usually Zircaloy or steel in modern constructions, or magnesium with a small amount of aluminium and other metals for obsolete reactors. Cladding prevents radioactive fission products from escaping from the fuel mixture into the coolant, contaminating it. Usually fuel rods are grouped into Fuel Assemblies (FAs), forming the core of a nuclear reactor (Fig. 2).

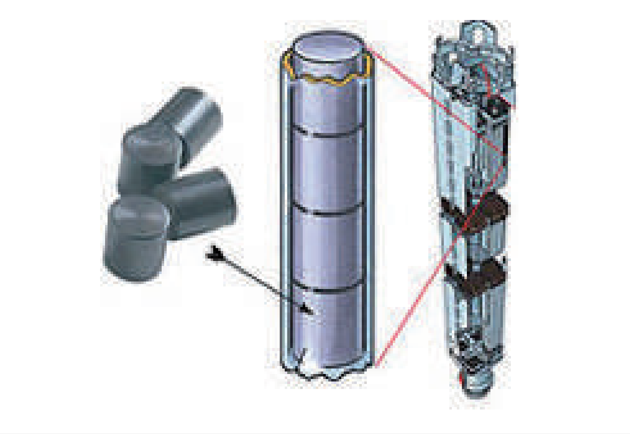


FIGURE 2 From fuel pellets to rods and assembly
Source: http://www.skb.se

During normal operations the fuel rods of nuclear power reactors are subject to internal stresses, which may lead to large dimensional changes or gross failure. Blistering, swelling and cracking are the most likely effects with which can lead to serious consequences. So far, deformations on fuel rods are inspected through a visual test.

Some optical technologies have been proposed but none of them has reached the necessary level of development to be applied in situ for the evaluation of rods integrity. The operation of a measurement device inside the vessels and pools of nuclear reactors, or in fuel storage facilities demands innovative solutions in terms of qualification to operate underwater and/or in radioactive, and/or contaminated environment. All these requirements have to be met without compromising the system performance.

The scenario for this Thematic Demo takes inspiration from several past real events, where an alert state was raised inside a nuclear facility as a consequence of deformations in one or more fuel rods.

For instance, on December 2012 Japan's nuclear regulatory authority confirmed a trouble with the fuel rods stored in a spent nuclear fuel pool at the Tokyo Electric Power Co.'s Kashiwazaki-Kariwa plant. A pair of fuel rods came into direct contact as a result of deformation in the bundle of fuel rods, leading the Nuclear Regulation Authority to determine that the fuel had likely been loaded into the reactor core "in an abnormal situation." An alert 1 level was then issued.

Purpose of the scenario

The exercise aims at both simulating the decisional flow for managing the deployment of an innovative inspection tool inside the storage pool, or the reactor pool of a nuclear reactor, and testing the reliability of the instrument and its performance. The technology of 3D laser scanner is gaining ground as an improved inspection tool for structural monitoring in several disciplines ranging from cultural heritage to Oil and Gas industry. The deployment of the device inside a sensitive area like a nuclear reactor plant comes with specific issues to take into account. Technical issues include the capability of the deployed device to withstand radiation doses compatible with the time required for acquiring the 3D model with the necessary spatial resolution. If the measurement is carried out in the storage pool on a neutron irradiated fuel rod, the gamma dose rate is expected to be of the order of 3kGy/h. In case of detection inside the reactor pool of the nuclear reactor, higher dose rates are expected. The scenario is intended for realizing a deployment condition of the sensor as closer as possible to the real situation. This also includes managing the decisional flow during the routine inspection campaign, with particular regard to actions to do in case a major fault is detected.

The undetected occurrence of cracks and deformations in the nuclear fuel rods is one of the main effects leading to critical situations in a nuclear power plant. Fuel swelling and thermal stresses are the main detrimental effects a fuel rod undergoes during its lifecycle.

If not timely detected these effects can lead in the worst cases to cladding breaches, which result in the release of fission products into the coolant, and even in fuel washout in the most severe cases. Such an event requires cleaning the primary coolant circuits and increases in outage time, and can have significant operating and financial impacts on the affected plants. IAEA reports [5] that during the 1994-2006 period in PWRs, an average of 13.8 out of 1000 FAs were found faulty with leaks (Fig. 3).

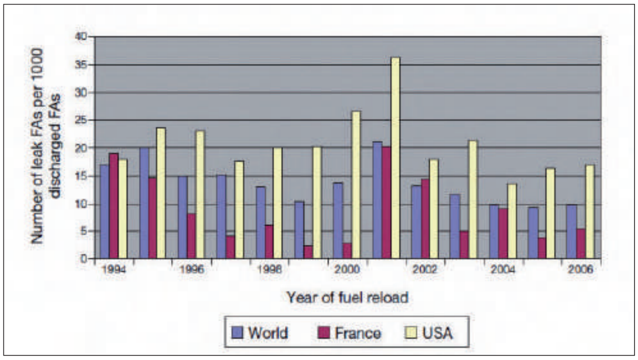


FIGURE 3 IAEA figures on FA found fault with leaks after inspection
Source: IAEA

The deployment of a 3D laser scanner inside the storage pool, and eventually in the reactor pool of the nuclear reactor, allows to reduce the downtime of planned or emergency inspections. Data can help the decision making process by the personnel appointed to run the plant during routine maintenance campaigns but also in the case of critical situations arising from emergencies.

The proposed methodology marks a significant improvement with respect to the current state of the art for assessing fuel rods deformation with most of the practices based on the inspector's skill rather than on quantitative and reliable data.

Scenario outline

TRIGA RC1 is a nuclear reactor for scientific purposes, with a limited power (1 MW) and not connected to the electrical grid, it being not intended for electricity generation. The reactor itself is located inside a research centre and does not resemble the operational environment of a big nuclear power plant. Nevertheless, the TRIGA RC1 nuclear reactor is well representative, despite its size, of all the issues that could emerge from an inspection campaign on fuel rods. The decisional flow leading to the deployment of the inspection sensor does not differ significantly from that in place in real high power production plants. From a technical point of view, the limited dimension of the storage pool and of the reactor pool makes the

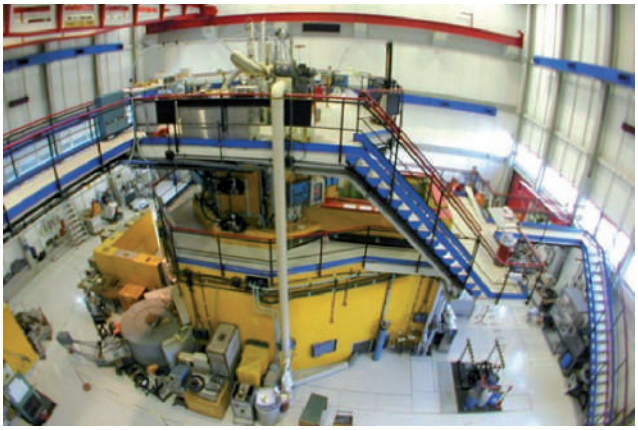


FIGURE 4 The TRIGA RC1 nuclear reactor

actuation of the 3D laser sensor in TRIGA RC1 more challenging than in a production plant (Fig. 4). This adds greater significance to the scientific-technical value of the demonstration action.

The event as a whole is intended for demonstrating that improved inspections with a remote laser system can be carried out in the sensitive area of a nuclear reactor, even without turning the plant off. This has deep implications when the scenario is rescaled to real power plants, which face high operative costs for each on/off cycle. The main benefit is the possibility to increase the rate of the inspections, their affordability and reliability. One of the distinctive features of the 3D laser scanner is the possibility to compare images taken at different times.

The simulated event during the exercise envisages a fabrication fault in one fuel rod that causes it to blister, or otherwise the occurrence of a deformation in the rod during the normal operation of the reactor. The laser device will detect this anomaly and the rod removal can be planned.

The fuel rods in TRIGA are made of a ternary alloy of Zr-U-H and are 72 cm in length with a diameter of 3.73 cm (Fig. 5).

First laboratory measurements and computer simulations show that 3D models of the rods can be acquired with a sub-millimetric spatial resolution with a sensor-target distance of 5 meters. This level of accuracy is appropriate for the inspection sensibility as required by end-users.

Conclusions

A vibrant research activity is underway at ENEA for carrying on, on September 2015, a Thematic Demo in the nuclear reactor TRIGA, demonstrating the capability of a 3D laser scanner to detect deformations in a fuel rod immersed in a wet contaminated environment. The action is supported by the European Project EDEN and the results will be evaluated by a panel of experts selected by the project coordinator from the list of the End-Users interested in the proposed technology. The synergetic collaborations between ENEA researchers with different skills and fields of competence have been instrumental to set up the exercise and will be the winning factor for its successful completion.

FIGURE 5 The TRIGA Fuel Rods

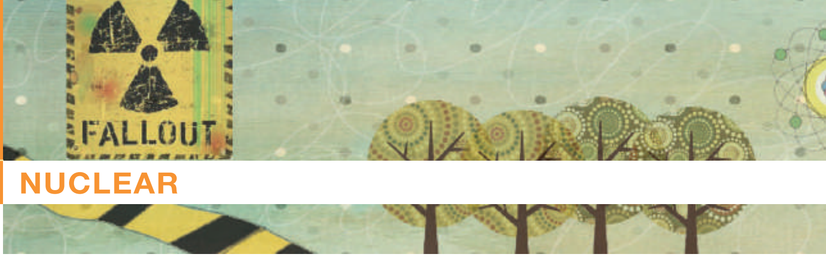
Luigi De Dominicis, Antonio Palucci, Mario Ferri de Collibus, Roberta Fantoni, Giorgio Fornetti, Massimo Francucci, Massimiliano Guarneri, Marcello Nuvoli
ENEA, Technical Unit for the Development of Applications of Radiation - Diagnostics and Laser Metrology Laboratory

Massimo Sepielli
ENEA, Technical Unit for Nuclear Fission Technologies and Facilities, and Nuclear Material Management

Mario Carta, Mario Palomba, Emilio Santoro
ENEA, Technical Unit for Nuclear Fission Technologies and Facilities, and Nuclear Material Management – Nuclear Research Reactor Laboratory

references & notes

[1] www.practice-fp7-security.eu
[2] www.decotessc1.eu
[3] www.eden-security-fp7.eu
[4] J. Cho, Y. Choi, K. Jeong, J. Shin, 2011, “Measurements of nuclear fuel rod deformation using an image processing technique”, in Nuclear Engineering and Technology, 43, 133-137.
[5] IAEA, 2010, “Review of Fuel Failures in Water Cooled Reactors”, IAEA Nuclear Energy Series, No. NF-T-2.1.



Scrittura e tracciamento di materiali radioattivi: una possibile soluzione hi-tech

Il presente articolo descrive la tecnica e gli strumenti per scrivere disegni invisibili su sottili etichette di metalli alcalini terrosi utilizzando una fonte di radiazione nell'estremo ultravioletto. È stato dimostrato sperimentalmente che il nostro metodo di scrittura rende praticamente impossibile la contraffazione di etichette realizzate con una pellicola sottile di fluoruro di litio e offre una protezione molto migliore rispetto alle tecniche anticontraffazione attualmente disponibili. I risultati di test preliminari di esposizione a raggi γ, *x* e β emessi da diversi radionuclidi, quali Co-60, Cs-137, Na-22, e Ba-133, si sono rivelati promettenti per poter usare queste etichette per tracciare materiali radioattivi, al fine di contrastare fenomeni che mettono a rischio la sicurezza, quali ad esempio lo smaltimento e il traffico illecito di scorie radioattive.

Marking and tracking radioactive materials: A possible hi-tech solution

We describe the technique and apparatus to write invisible patterns on thin tags of alkali halides by using an extreme ultraviolet radiation source. We have experimentally demonstrated that lithium fluoride thin-films tags written using this method are almost impossible to counterfeit, and offer a much better protection than the available anti-counterfeiting techniques. The results of preliminary tests of exposure to γ-, *x*- and β-radiation emitted by several radio-nuclides, like Co-60, Cs-137, Na-22, and Ba-133 are promising for the use of these tags to track radioactive materials, in order to fight phenomena impacting security, like the illicit disposal and traffic in radioactive waste.

DOI: 10.12910/EAI2014-97

■ *S. Bollanti, P. Di Lazzaro, F. Flora, L. Mezi, D. Murra, A. Torre, F. Bonfigli, R.M. Montereali, M.A. Vincenti*

Introduction

Counterfeiting is a global problem that has major social and economic consequences [1]. In a recent update [2] the Organization for Economic Co-operation and Development has estimated in USD 250 billion in 2007 the worldwide value of international trade in counterfeit goods, with an impressive growth rate of USD 25 billion/year.

The range of counterfeited products has broadened from luxury objects to products directly impacting on health and safety, like food, pharmaceutical products and automotive/aerospace spare parts, as well as security, like the illegal trade and disposal of radioactive waste coming from both civilian (power plants, hospitals, industries) and military uses.

■ **Contact person: Paolo Di Lazzaro**
paolo.dilazzaro@enea.it

As a consequence, anti-counterfeiting (AC) technologies are continuously evolving, extending their applications to identification of the origin of objects or certificates, traceability and identification of paper currency, identity/credit/debit cards, forensic documents, critical/strategic components, dangerous wastes, pharmaceutical products, artworks.

Many AC techniques based on high-tech tagging have been developed, like fluorescent inks (currently used, e.g., in banknotes), thermo-chromic inks, demetallized hot stamping foils, holograms, diffractive foils, laser engraving (writing inside glasses) and radiofrequency identifiers. However, each of these techniques has its own effectiveness and lifetime limited by a variety of factors, including the ability of counterfeiters to replicate the technique, so that a continuous innovation of AC technologies is needed. Moreover, none of the above techniques contemporarily matches a demanding way for a difficult-to-replicate marking and a simple control reading, being at the same time respectful of the privacy issue.

We propose here an invisible marking technology to tag goods/objects whose counterfeiting may impact on both safety and security. After a description of our technology, we present experimental tests to check its application in marking and tracking radioactive materials.

Background

At the ENEA Research Centre in Frascati we have developed expertise in the field of extreme ultraviolet (EUV) and soft *x*-rays generation and applications [3]. In particular, we operated a plasma source driven by two different XeCl excimer lasers. The short-wavelength radiation λ (4 nm < λ <60 nm) emitted by the laser-plasma source is used in different fields, ranging from soft *x*-ray microscopy to radiobiology, from micro-radiography to microelectronics and photonics. Based on our laser-plasma source, we have developed an apparatus for EUV projection lithography, named MET-EGERIA, which is able to print a sub-100-nm-resolution pattern on polymethylmethacrylate (PMMA) resist [4, 5].

Recently, we operated a discharge-produced-plasma source (DPP), which can deliver EUV pulses with energy/solid angle of 20 mJ/ster in the 10-20 nm wavelength spectrum and 60 mJ/sr/shot in the full EUV range, working up to 20 Hz repetition rate [6]. The DPP is particularly suitable to irradiate large-sized targets in the near field with a higher yield vs. laser-plasma source, thus showing its superiority in the EUV contact lithography irradiations.

In specific materials, like alkali halides, EUV radiation can generate electronic point defects, known as "colour centres", which make them luminescent under selective optical pumping [7]. In the case of lithium fluoride (LiF) this modification is permanent at room temperature and the photoluminescence of radiation-induced defects is in the visible spectral range.

Thanks to the very short penetration depth of EUV in most materials, the coloured layer in LiF is so thin (~50 nm) to potentially allow for a very high resolution patterning. A film of LiF can be deposited by thermal evaporation [8] directly on the goods to be protected/traced, or on a tag to be stuck on them. After a suitable EUV irradiation dose, the stored pattern is invisible to the naked eye, and the emitted photoluminescence can be observed only through a suitable optical filter after the colour centres are excited by a spectrally selected illumination.

An example of high-resolution luminescent patterns in a field of about (0.5 x 0.5) mm^2, obtained using a projection EUV microlithography tool, is shown in Figure 1. This is a complex and expensive writing tool, which requires skill and experience in the fields of EUV sources and EUV optics.

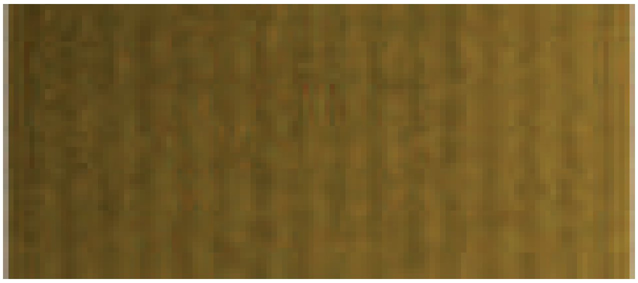


FIGURE 1 Luminescent patterns stored on a LiF film deposited by thermal evaporation on a glass substrate at ENEA [8], obtained by the MET-EGERIA described in [4, 5]. The pattern period is 2.2 micrometers

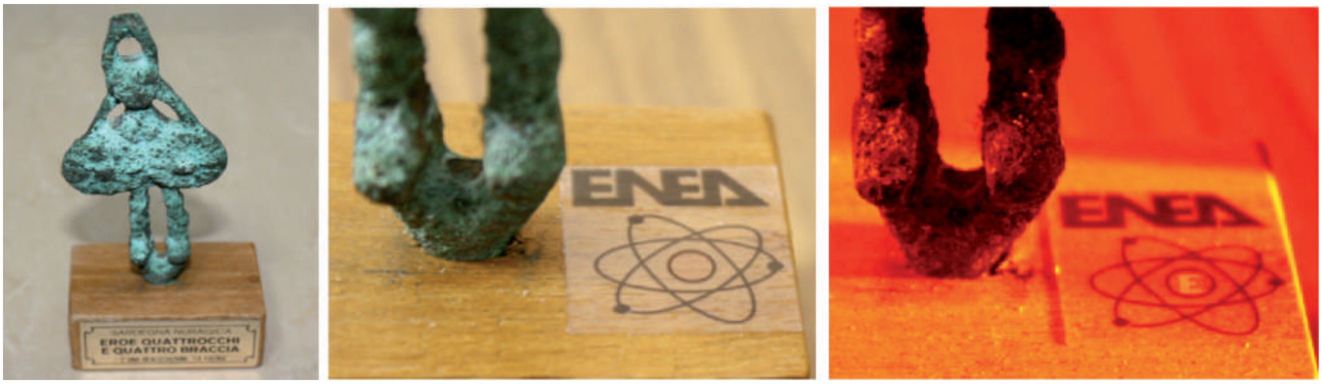


FIGURE 2 Left: Copy of an archaeological bronze statue, known as “hero four-eyes and four-arms”, height: 11 cm; Middle: The transparent and adhesive tag based on a LiF film stuck on the wood base of the statue; Right: The letter ‘E’ patterned by EUV radiation appears when using the patented reading technique
Source: [9]

The invisible marking

Figure 2 shows a LiF film tag patterned by EUV radiation using a contact mask, in this specific case for artwork protection. The letter E becomes visible only by the specific optical excitation and spectrally selected fluorescence spectra.
The apparent similarity with the behaviour of some fluorescent inks fails at a deeper analysis, thanks to the low absorption of colour centres in the ultraviolet, which, on the contrary, is strongly absorbed by most inks, see Figure 3. A simple, differential spectral reading system can thus definitely distinguish between a mark written by our technique and the same mark written by fluorescent ink.
The capability to grow LiF thin films [10] even on plastic substrates allows to develop adhesive tags to stick on the items to be protected and/or traced.
The security level of our technology can be further increased by the digital encoding of the image, by using the current state-of-the-art cryptography techniques. In this case, the control relies not only on the physical reading of the image, but also on its decoding with the appropriate digital key/algorithm [9].
We can further increase the security level of our technology by growing alkali halide films in a series of thin layers, each separated by non-luminescent materials, with a variable tapered thickness. By so doing, after irradiation by ionizing radiation, the energy of the ionizing radiation affects the luminescence ratio of the different layers, and therefore a mark imprinted with an ionizing radiation having a different spectral energy with respect to a pre-determined one can be identified.
ENEA has filed two patents about the invisible marking system [11].

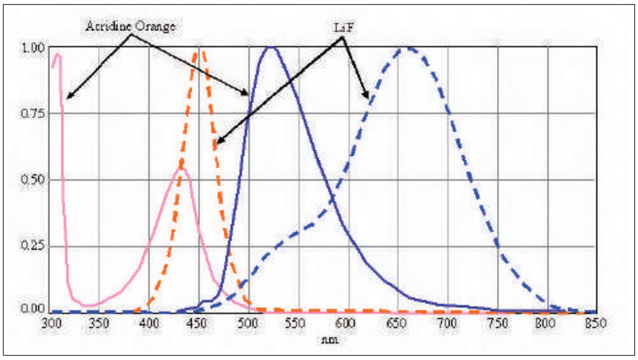


FIGURE 3 Optical absorption and emission spectra of LiF colour centres (dashed lines) and of Acridine orange (continuous lines) in the range 300 nm - 850 nm. Acridine orange is one of the dyes having the most similar absorption and emission spectra vs. LiF
Source: [9]

Is our invisible marking suitable to security-related applications?

In the past, we tested our invisible writing technique to produce AC tags able to protect identity/payment cards and electronic components [12] as well as artworks [9]. Here we discuss the potential use of our technology as identification marks for tracking radioactive substances, which may impact security issues. In fact, a critical field of marking application is related to the traceability of radioactive waste, coming from both civilian (power plants, hospitals, industry) and military uses, in order to trace their origin and then fight the phenomena which impact on security, like their illicit traffic or disposal.

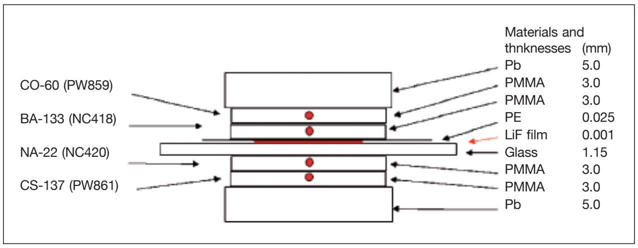


FIGURE 4 Schematic of the irradiation setup of the LiF film patterned with the invisible EUV-marking. The film was sandwiched between several radio-nuclides and exposed to a total dose of 1,700 Gy during 40 days of continuous exposure

Upon request by GIS (Special Intervention Group of Carabinieri military police) we made preliminary irradiation experiments to check if the ionizing radiation emitted by radioactive substances was able to alter the visibility of our marking. To this end, we prepared two LiF thin films deposited on a glass substrate, patterned by irradiation with EUV light through a hexagonal grid. We irradiated one of these films with a total radiation dose of 1.7×10^3 Gy (1 Gy = 1 J/kg) during 40 days of exposure, i.e., with a maximum rate of 1.33 Gy/hour. The exposure was performed by adding γ-, x- and β-radiation contributions from several radio-nuclides, namely Co-60, Ba-133, Na-22, Cs-137. Note that Co-60 and Cs-137 are widely used in industrial radiography (to measure weld and weld overlays, castings, forgings, valves and components, pressure vessels, structural steel, aircraft structures); Co-60 is also used in cancer therapy, whilst Ba-133 is commonly used in manufacturing to measure, e.g., the thickness of metal components and coatings, or the moisture content in manufactured products [13]. In addition, all the above radio-nuclides are used in oil and gas industry [14].

The schematic of the irradiation setup is shown in Figure 4, and the main results are reported in Figure 5, where EUV-marked film is shown before and after irradiation (Figs. 5a and 5b, respectively), as observed by an optical microscope under the same illumination

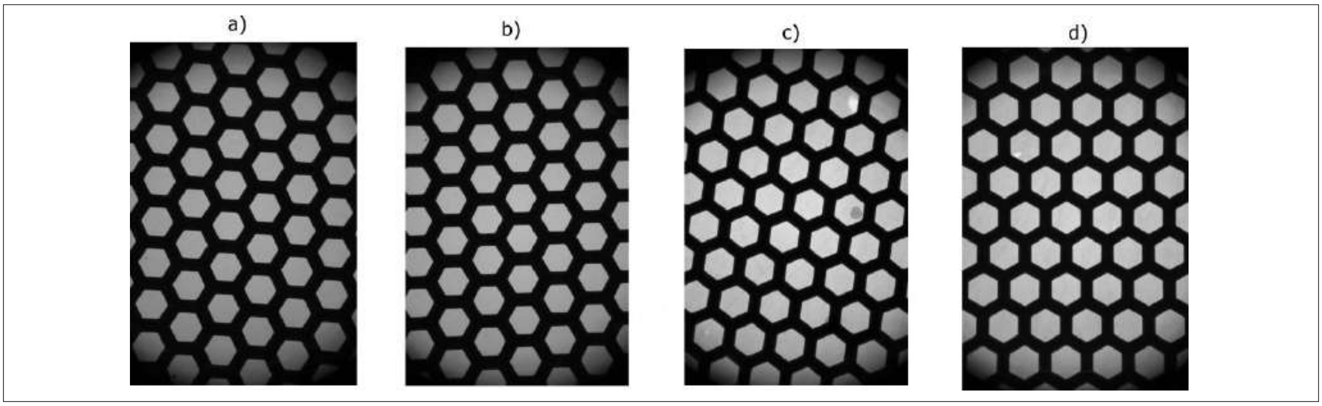


FIGURE 5 Microscope views of the invisible pattern on the LiF films evidenced by the patented reading technique. The period of the hexagonal pattern is about 0.05 mm. From left to right: a) Before irradiation; b) After 40 days of irradiation with a total dose of 1700 Gy; c) Reference sample, not irradiated; d) The same reference sample after 40 days

conditions of a reference unexposed film (see Figs. 5c and 5d).

It appears that the prolonged contact with radioactive materials and consequent exposure did not alter the contrast of the image, and the pattern, still invisible under normal illumination, does not show any detectable difference with respect to the reference pattern on unexposed film (cf. Figs. 5b and 5d).

Accurate and systematic spectral investigations of colour centres in γ-irradiated lithium fluoride thin films in [15, 16] have confirmed that the colour centre photoluminescence generated by a dose of 10^3 Gy is not sufficient to change the contrast of the EUV marking in Figure 5, whilst at a very high dose of 10^6 Gy the photoluminescence of the radiation-induced defects grows to a level that could make it difficult to observe the EUV marking.

Then, a careful choice of the LiF film characteristics (i.e., reducing the film thickness) and an accurate control of their structural, morphological and optical properties are essential to assure the capability of the AC tag behaviour for tracking standard radioactive substances.

Towards the market: durability and production yield

When seeking for security-related uses of our technology, an important issue is the durability of the invisible writing on AC tags. In general, LiF is a rugged material, hard and almost non-hygroscopic. Our tests show that the irradiated LiF films can be touched many times without significantly damaging or altering the visibility of the pattern, as detailed in [12]. When the tags are exposed to severe conditions (heavy and uncontrolled scratching or abrasions), a protecting film can be applied on the tag.

From the production point of view, there are several parameters that influence the number of tags written per unit time, including the time to accurately align the contact masks on tags, the maximum number of tags that can be irradiated in the same run, and the area to be irradiated (which depends on the size of the pattern). When using a commercial EUV source delivering a moderate 100 W average power in the EUV [17], a conservative estimation gives a potential production yield of about 50-100 tags/hour, each tag having a patterned area of 0.4 cm^2.

Conclusions

ENEA has developed and patented a new anti-counterfeiting/tracking technology based on EUV lithography on radiation-sensitive luminescent materials. An arbitrary pattern can be transferred as an invisible image on thin tags based on alkali halides, which in turn can be put on or embedded in any object to be protected or traced. A compact and cheap device can read the luminescent image and check the authenticity and/or the origin of the tags.

Our writing tool is complex and expensive, and requires a skilled team to be optimized. As a consequence, it is highly unlikely that a counterfeiter could build and operate a similar writing tool. On the other hand, the reading system is cheap and simple so that everyone can easily check the presence of invisible patterns to verify if the good is genuine or to check the origin of the material if interested on its tracking.

The complexity and safety level of our hidden patterns can be further enhanced and adjusted by encoding patterns by cryptography techniques, and/or by growing the fluorescent film as a series of thin layers, each separated by non-luminescent materials with variable thickness, as detailed in [11]. The ENEA technology can be used alone, or in conjunction with other anti-counterfeiting/tracing methods.

In previous papers we have demonstrated the feasibility of the application of this technology to artworks [9], to credit/debit cards and electronic components [12], also showing that our AC tags cannot be detached from the original object and stuck on another one, since in this case the pattern becomes visible.

In this paper, we have shown how the exposure of these AC tags with radioactive materials up to a total dose of 1,700 Gy does not alter the contrast of the invisible EUV pattern, see Figure 5. As a consequence, our tags are promising candidates as identification marks for tracking radioactive substances, thus being potentially effective to fight the illicit traffic and disposal of radioactive materials coming from both civilian (power plants, hospitals, industries) and military uses.

As regards the market, a conservative estimation shows that a production of about 50-100 tags/hour can be achieved.

The protection level of our technology can be evaluated by the following standard criteria:

- very high cost to break;
- high probability to detect a clone;
- very low probability of false negatives;
- no privacy risks.

Concerning vulnerabilities, at the moment we are not able to find practical ways to fool the product authentication/tracking.

Sarah Bollanti, Paolo Di Lazzaro, Francesco Flora, Luca Mezi, Daniele Murra
ENEA, Technical Unit for the Development of Applications of Radiation - Radiation Sources Laboratory

Amalia Torre
ENEA, Technical Unit for the Development of Applications of Radiation - Mathematic Modelling Laboratory

Francesca Bonfigli, Rosa Maria Montereali, Maria Aurora Vincenti
ENEA, Technical Unit for the Development of Applications of Radiation - Photonics Micro and Nanostructures Laboratory

references & notes

[1] http://www.oecd.org/industry/industryandglobalisation/2090589.pdf

[2] http://www.oecd.org/industry/industryandglobalisation/44088872.pdf

[3] S. Bollanti, F. Bonfigli, E. Burattini, P. Di Lazzaro, F. Flora, A. Grilli, T. Letardi, N. Lisi, A. Marinai, L. Mezi, D. Murra, C.E. Zheng, 2003, "High efficiency, clean EUV plasma source at 10-30 nm, driven by a long pulsewidth excimer laser", in Applied Physics B, 76, 277-284.

[4] S. Bollanti, P. Di Lazzaro, F. Flora, L. Mezi, D. Murra, A. Torre, 2008, "First results of high-resolution patterning by the ENEA laboratory-scale extreme ultraviolet projection lithography system", in European Physics Letters, 84, 58003 p1-58003 p5.

[5] P. Di Lazzaro, S. Bollanti, F. Flora, L. Mezi, D. Murra, A. Torre, 2009, "Excimer-laser-driven EUV plasma source for single-shot projection lithography", in IEEE Transactions of Plasma Science, 37, 475-480.

[6] L. Mezi, F. Flora, "La Sorgente "DPP" di radiazione nell'estremo ultravioletto a scarica elettrica in gas rarefatto Principi fisici, caratterizzazione ed ottimizzazione", Rapporto Tecnico ENEA RT/2012/15 http://opac.bologna.enea.it:8991/RT/2012/2012_15_ENEA.pdf

[7] G. Baldacchini, S. Bollanti, F. Bonfigli, F. Flora, P. Di Lazzaro, A. Lai, T. Marolo, R.M. Montereali, D. Murra, A. Faenov, T. Pikuz, E. Nichelatti, G. Tomassetti, A. Reale, L. Reale, A. Ritucci, T. Limongi, L. Palladino, M. Francucci, S. Martellucci, G. Petrocelli, 2005, "Novel soft x-ray submicron imaging detector based on point defects in LiF", in Review Scientific Instruments, 76, 113104, 1-12.

[8] R.M. Montereali, "Point defects in thin insulating films of lithium fluoride for optical microsystems", 2002, in Handbook of Thin Film Materials, H.S. Nalwa, ed., Academic Press, vol 3: Ferroelectric and Dielectric Thin Films, Ch.7, 399-431.

[9] S. Bollanti, P. Di Lazzaro, F. Flora, L. Mezi, D. Murra, A. Torre, F. Bonfigli, R.M. Montereali, M. Vincenti, 2012, "Is this artwork original or is it a copy? The answer by a new anti-counterfeiting tag", in Energia, Ambiente e Innovazione, special issue on Knowledge, Diagnostics and Preservation of Cultural Heritage, 162-168, available online at http://www.enea.it/it/produzione-scientifica/pdf-eai/speciale-cultural-heritage/25-is-this-artwork-pdf

[10] M.A. Vincenti, R.M. Montereali, G. Messina, E. Nichelatti, A. Mancini, A. Rufoloni, 2013, "Growth and characterization of thermally-evaporated lithium fluoride thin films for radiation detectors", ENEA Technical Report RT/2013/22/ENEA, http://hdl.handle.net/10840/4858

[11] European patent: "Invisible writing method based on lithography of luminescent materials, relevant reading method and anti-counterfeiting marking system" EP 2266115 (2010). Italian patent: "Method for the detection of micrometric and sub-micrometric images obtained by means of ionizing radiations" IT 1.337.672, 2002.

[12] P. Di Lazzaro, S. Bollanti, F. Flora, L. Mezi, D. Murra, A. Torre, F. Bonfigli, R.M. Montereali, M.A. Vincenti, 2012, "Extreme ultraviolet marking system for anti-counterfeiting tags with adjustable security level", in XIX International Symposium on High-Power Laser Systems and Applications 2012, Proc. SPIE, Vol. 8677, 86770T, DOI: 10.1117/12.2010400

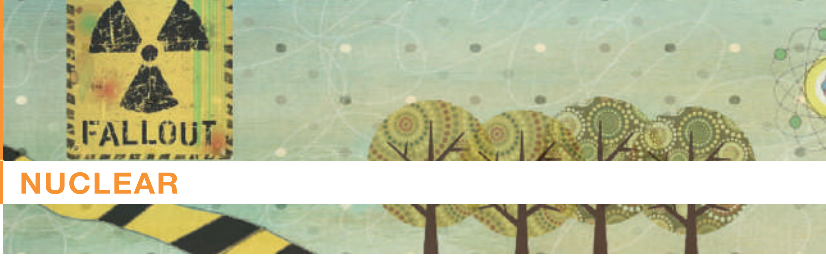
[13] See, e.g., www.epa.gov/radiation/source-reduction-management/applications.html

[14] F.A. Jarad, 2008, "Application of Radiation Sources in the Oil & Gas Industry and Shortages in their Services", Int. Symposium on Peaceful Applications of Nuclear Technology, available online at http://procurement.kau.edu.sa/Files/320/Researches/47387_18847.pdf

[15] R.M. Montereali, T. Marolo, M. Montecchi, E. Nichelatti, 2012, "Spectral Investigation of Colour Centres in Gamma Irradiated Lithium Fluoride Thin Films", in Nuclear Instruments and Methods B, 268, 2866-2869, see http://dx.doi.org/10.1016/j.nimb.2010.03.020

[16] M. Montecchi, S. Baccaro, E. Nichelatti, F. Bonfigli, T. Marolo, R.M. Montereali, 2002, "Point Defects in Lithium Fluoride Films Induced by Gamma Irradiation", in Proc. 7th International Conference on Advanced Technology and Particle Physics (ICATPP-7), M. Barone, E. Borchi, J. Huston, C. Leroy, P.G. Rancoita, P. Riboni, R. Ruchiti Eds., World Scientific, 819-825.

[17] The main Companies producing high average power EUV sources are Bruker (http://www.bruker-est.com/xuv.html), Ushio and its subsidiary Xtreme (http://xtremetec.com/; http://www.xtremetec.de/who/company.html).



Come contrastare la dispersione di materiale radioattivo: le competenze ENEA

La dispersione di materiale radioattivo potrebbe derivare da un incidente radiologico o da un atto doloso. In entrambi i casi siamo alla presenza dello stesso scenario ma con importanti differenze che richiedono un approccio completamente differente. L'aspetto più rilevante è la possibilità di prevedere il primo tipo di evento e di preparare una risposta sito-specifica, mentre nel secondo caso è possibile unicamente adottare un approccio di tipo generico.
Nel presente articolo è illustrato l'approccio generico proposto dagli esperti ENEA in caso di dispersione di materiale radioattivo dovuta ad atto doloso. Sono inoltre proposti e discussi l'analisi provvisoria e l'approccio di risposta. Sono esposti gli strumenti, gli impianti e le competenze dell'Agenzia ENEA, che rendono possibile l'impresa.

Facing dispersion of radioactive material: ENEA's skills

The dispersion of radioactive material could derive either from a radiological incident or from a malevolent act. Both situations appear to present the same scenario but there are important differences that require a completely different approach. The most important aspect is the possibility of foreseeing the first kind of event and of preparing a specific-site response, while in the case of a malevolent act only a general approach is possible. This paper shows the general approach proposed by ENEA experts to face a dispersion of radioactive material due to a malevolent act. The provisional analysis and the responding approach are proposed and discussed. The tools and the facilities available in the Agency are considered, together with ENEA skills that make the enterprise possible.

DOI: 10.12910/EAI2014-98

■ *S. Sandri*

Introduction

In a terroristic attack radioactive materials could be used in many ways. This kind of event is often called "radiological attack" and means the spreading of radioactive material with the intent to do harm. Radioactive materials are used every day in laboratories, medical centers, food irradiation plants, and for industrial uses; if stolen, or otherwise acquired, many of these materials could be used in a "radiological dispersal device" (RDD). A "dirty bomb" is one type of RDD that uses a conventional explosion to disperse radioactive material over a targeted area. RDDs could also include other means of dispersal such as placing a container of radioactive material in a public place, or using an airplane to disperse

■ Contact person: Sandro Sandri
sandro.sandri@enea.it

powdered or aerosolized forms of radioactive material. Another kind of radiological device that could be used by terrorists is the so called RED (Radiation Emission/ Exposure Device), a weapon of terror whereby a high-intensity radiation source is placed in a public area to expose those individuals in close proximity. Prolonged exposure to a high intensity source may lead to acute radiation syndrome (ARS) or to cutaneous radiation syndrome (CRS), or radiation burns.

Many Italian institutions, with national or local relevance, are in the position to be identified as the potential responders to a radiological attack. Nevertheless the majority of these institutions expressed the need for assistance in identifying the most important actions that should take place when responding to an RDD.

The Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA) develops activities devoted to research, innovation technology and advanced services in the fields of energy, especially nuclear. One of ENEA's tasks is to provide support to the Ministry for Economic Development (MSE), Regions, and local bodies in the specific field of interest, and also in responding to radiological events.

Typical areas of intervention for the Agency are: developing methods to measure and control the radiation and contamination; providing specific information to citizens, public administrations, enterprises and economic operators.

ENEA is already considered the National Focal Point for the assistance to operators in the various phases of radioactive material transport. In this framework, the Agency assists those who need help in transporting radioactive materials within the national territory, even if just transiting. It also acts as an interface between the National Authorities and the IAEA Secretariat during all shipment phases. In addition, for many years ENEA has hosted an Integrated Service for the management of non-electro-nuclear radioactive waste spread all over Italy, which include low- and medium-level medical radioactive sources as well as high-activity sealed radioactive sources. ENEA's Integrated Service is responsible for radioactive waste collection, transport, characterization, storage, treatment and conditioning. Since 2007, pursuant to Legislative Decree No. 52 of 6 February 2007, the Integrated Service is also responsible for orphan sources (radioactive sources for which origin cannot be determined). ENEA acts in these areas with specific Technical Units. Those mainly involved in the research and support related to radiological attacks are the Technical Unit for the Development of Applications of Radiations (UTAPRAD) and the Radiation Protection Institute (IRP). The staff of the above Units owns unique expertise and intervention skills and can meet all kinds of needs associated with the use of ionizing radiation also in a malevolent action.

The high-quality consultation provided by ENEA experts includes the identification of the needed tasks, the initial guidance for the first after-event hours, the national, regional, and state/ local agency contacts and the assistance with radiological emergency response capabilities.

The radiological dispersal devices

The terms dirty bomb and RDD are often used interchangeably in the media. Any kind of dirty bomb is in no way similar to a nuclear weapon or nuclear bomb. A nuclear bomb creates an explosion that is millions of times more powerful than that of a dirty bomb. The cloud of radiation from a nuclear bomb could spread tens to hundreds of square miles, whereas an RDD's radiation could be dispersed within a few blocks or miles from the explosion. A dirty bomb cannot be considered a "Weapon of Mass Destruction" but it could be a "Weapon of Mass Disruption," where contamination and anxiety are the terrorists' major objectives.

Most RDDs would not release enough radiation to kill people or cause severe illness. The conventional explosive in the bomb itself would be more harmful to individuals than the dispersed radioactive material. However, depending on the situation, an RDD explosion could create fear and panic, contaminate property, and require potentially costly cleanup. Making prompt, accurate information available to the public may prevent the panic sought by terrorists. Nevertheless, terrorist use of an RDD is considered far more likely than using a nuclear explosive device. It is designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Such RDDs appeal to terrorists because they require limited technical

Common radioactive sources

Gamma emitters

Cobalt-60 (Co-60): cancer therapy, industrial radiography, industrial gauges, food irradiation.
Cesium-137 (Cs-137): same uses as Cobalt-60 plus well logging. Iridium-192 (Ir-192): industrial radiography and medical implants for cancer therapy.

Beta emitter

Strontium-90 (Sr-90): radioisotope thermoelectric generators (RTGs), which are used to make electricity in remote areas.

Alpha emitters

Plutonium-238 (Pu-238): research and well logging and in RTGs for space missions.
Americium-241 (Am-241): industrial gauges and well logging.

knowledge to build and deploy compared to a nuclear device. Also, the radioactive materials in RDDs are widely used in medicine, agriculture, industry and research, and are easier to obtain than weapons grade uranium or plutonium. On the other hand, it is very difficult to design an RDD that would deliver radiation doses high enough to cause immediate health effects or fatalities in a large number of people. Therefore, experts generally agree that an RDD would most likely be used to contaminate facilities or places where people live and work, disrupting lives and livelihoods. Experts are convinced as well that the primary purpose of terrorist use of an RDD is to cause psychological fear and economic disruption.

An RDD could cause fatalities from exposure to radioactive materials, depending on many aspects. The speed at which the area of the device detonation is evacuated and how successfully people are recovered at sheltering-in-place are the main parameters on which the event outcome is based. In any case the number of deaths and injuries from an RDD might not be substantially greater than from a conventional bomb explosion.

The size of the affected area and the level of destruction caused by an RDD would depend on the sophistication and size of the conventional bomb, the type of radioactive material used, the quality and quantity of radioactive material, and the local meteorological conditions, primarily wind and precipitation. As a result, the area affected could be placed off-limits to the public for several months during cleanup efforts.

Preparing to the impact

In order to be prepared for facing an RDD impact, it is important to understand the meaning of a specific dose level. The effective dose of 1 mSv is the limit imposed worldwide to guarantee that people not working with radiations will receive an insignificant dose due to the artificial use and production of ionizing radiations. It is not directly correlated with the human safety. In fact normal background radiation varies from place to place but delivers a worldwide average effective dose near 2.4 mSv/year. This implies that an annual dose of 1 mSv is not harmful for humans, who are used to live in a more radioactive environment. The International Commission on Radiological Protection (ICRP), that is the primary international body in protection against ionizing radiation, states that *the most adverse health effects of radiation exposure may be grouped in two general categories: deterministic effects (harmful tissue reactions) due in large part to the killing/malfunction of cells following high doses; and stochastic effects, i.e., cancer and heritable effects involving either cancer development in exposed individuals owing to mutation of somatic cells, or heritable disease in their offspring owing to mutation of reproductive (germ) cells [1].* The induction of deterministic effects is characterized by a threshold dose. Below the threshold the radiation damage of a critical tissue is not sustained enough and the injury could not be expressed in a clinically relevant form. Above the threshold dose the severity of the injury, including impairment of the capacity for tissue recovery, increases with the dose.

In the dose range up to around some hundreds of millisievert no tissues are judged to express clinically relevant functional impairment, and therefore there are not deterministic effects. An average threshold for the

Dose definition

Only the amount of energy from any type of ionizing radiation that is imparted to (or absorbed by) the human body can cause harm to health.
To look at biological effects, we must know (estimate) how much energy is deposited per unit mass of the part (or whole) of our body which the radiation is interacting with.

The international (SI) unit of measure for absorbed dose is the gray (Gy), which is defined as 1 joule of energy deposited in 1 kilogram of mass. The old unit of measure for this is the rad, which stands for "radiation absorbed dose." 1 Gy = 100 rad.

Equivalent dose represents the biological effect to a specific organ or tissue and depends not only on the amount of the absorbed dose but also on the intensity of ionisation in living cells caused by different types of radiation.
Neutron, proton and alpha radiation can cause 5-20 times more harm than the same amount of the absorbed dose of beta or gamma radiation.
The unit of equivalent dose is the sievert (Sv). The old unit of measure is the rem. 1 Sv = 100 rem.

Effective dose is the numerical representation of the biological effect to the whole body and is obtained by adding the equivalent doses to all the organs and tissues weighted by specific coefficients.
The unit of effective dose is the sievert (Sv). The old unit of measure is the rem. 1 Sv = 100 rem.

deterministic effects induction could be fixed around 500 mSv [2], even if some minor tissue reactions (like skin erythema) could be observed in some persons exposed in the dose range from 100 to 500 mSv.
Stochastic effects are health effects that occur randomly and for which the probability of the effect occurring, rather than its severity, is assumed to be a linear function of dose without threshold. In the case of cancer, epidemiological and experimental studies provide evidence of radiation risk albeit with uncertainties at doses about 100 mSv or less. In the case of heritable diseases, there is no direct evidence of radiation risks to humans, yet experimental observations argue convincingly that such risks for future generations could be real. Coming back to the radiological effects that could be expected for the individuals living in the area of an RDD influence, the doses we are generally dealing with should be ranging from less than 1 mSv to some hundreds of millisievert. People staying closer to the strike point could be exposed to higher dose levels, but these persons should be in a small number, not higher than few tenths of individuals.
On the other hand, it has to be noticed that the World Health Organization considers an individual dose of 500 mSv/year acceptable for emergency work [3]. Therefore in general, after an RDD impact, the health effects to the involved individuals are expected to be restricted to the stochastic injuries for most of them, with minor deterministic tissue reactions for those exposed to doses close to 500 mSv or higher.
In general, there is no way of knowing how much warning time there will be before an attack by terrorists using an RDD, nor how high the maximum dose level due to the attack will be, so being prepared in advance and knowing what to do and when is extremely important.
To prepare for an RDD event it is important to build an Emergency Supply Kit, including items like non-perishable food, water, a battery-powered or hand-crank radio, extra flashlights and batteries, a roll of duct tape and scissors.
Taking shelter during an RDD event is absolutely necessary. There are two kinds of shelters, blast and fallout. Blast shelters are specifically constructed to offer some protection against blast pressure, initial radiation, heat, and fire. But even a blast shelter cannot withstand a direct hit from a nuclear explosion.
Fallout shelters can be any protected space, provided that the walls and roof are thick and dense enough to absorb the radiation given off by fallout particles.
The experts of the ENEA Agency use specific computer codes to prepare various scenarios for the calculation of the dispersion of the bearing radionuclides in the atmosphere [4]. The calculations also provide the consequent dose to the most exposed individual and the collective dose. Many scenarios can be investigated

and the results are available to be used by the competent authorities. Typical commercial computer codes used in this kind of simulations are Hotspot [5] and Rascal [6]. The special features of these two codes are complementary, giving the results useful for preventing the major damages and for applying the best recovering measures. Participation to International exercises like those of the INEX series (international nuclear emergency exercises), organized under the OECD Nuclear Energy Agency's (NEA) Working Party on Nuclear Emergency Matters (WPNEM) [7], is extremely important for testing, investigating and improving national and international response arrangements for nuclear accidents and radiological emergencies. ENEA experts participate to the organization of this kind of international workshops improving their experience and comparing their knowledge with that of other high level professionals.

Facing the impact

Protection from radiation is afforded by:

- minimizing the time exposed to radioactive materials;
- maximizing the distance from the source of radiation;
- shielding from external exposure
- protecting from ingesting or inhaling radioactive material.

While the explosive blast is immediately obvious, the presence of radiation is recognized only by trained personnel with specialized equipment on the scene. Whether the event occurs indoors or outdoors, it would be safer to assume radiological contamination has occurred, particularly in an urban setting or near other likely terrorist targets. Avoiding or limiting internal exposure is important to protect from inhaling the radioactive dust resulting from the explosion. The best solution is to seek shelter from any location (indoors or outdoors), but if dust or other contaminants are manifest in the air, also other precautions could be used. Some of them are very simple, like breathing through the cloth of a shirt or of a coat to limit the exposure. Anyway also avoiding breathing radioactive dust, the proximity to the radioactive particles may still result in some radiation exposure (external).

If the explosion or radiological release occurs inside, individuals must get out immediately and seek safe shelter. Those who are outdoors have to seek shelter indoors immediately in the nearest undamaged building. If appropriate shelter is not available, people must cover their nose and mouth and move as rapidly as they can upwind, away from the location of the explosive blast. If the event occurs outside, individuals who are indoors must manage to turn off ventilation and heating systems, to close windows, vents, fireplace dampers, exhaust fans, and clothes dryer vents. It is therefore important to seek shelter immediately, preferably underground or in an interior room of a building, placing as much distance and dense shielding as possible between the refuge and the crucial point in which the radioactive material originates. After finding safe shelter, those who may have been exposed to radioactive material should decontaminate themselves following these steps: remove and bag potentially contaminated clothing; isolate the bag away from people; shower contaminated individuals thoroughly with soap and water; then, after officials indicate it is safe to leave shelter, seek medical attention. Table 1 shows a possible action program for the first 12 hours after the impact.

The ENEA Institute of Radiation Protection (IRP), with the skills and equipment of its laboratories distributed in five ENEA research centers, is able to supply advanced technical measurements, dose assessment and radiological safety advice to the people involved in the event. Among these services provided by ENEA IRP the monitoring of the contamination is one of the most advanced. It is mainly aimed at the individual monitoring of internal contamination by radionuclides and takes advantage of the application of the most up-to-date methods of analysis and measurement for the determination of radioactivity in the human body (in vivo), in the biological samples (in vitro measurements), and in many other kinds of material mixtures. Actually, at the moment, ENEA IRP laboratories are the only one in Italy able to address every need in the field of individual monitoring for internal dosimetry.

Potential safety implications

People closest to the point of the RDD impact would be the most likely to sustain injuries due to the explosion.

Decision exposure rate (microSv/h)	Radiation Zones (microSv/h)	Activities	Total accumulated stay time for first 12 Hrs
Background	Uncontrolled	No restrictions. The best location for Incident Command and decontamination activities.	Unlimited
10	Low Radiation Zone 10 - 100	If feasible, restrict access to essential individuals. Initial decontamination of first responders should occur near the outer boundary of this area. Uninjured personnel within this zone at the time of the RDD explosion can be directed to proceed directly home to shower if resources do not permit contamination surveying at the scene.	Full 12 Hours
100	Medium Radiation Zone 100 – 1000	Restrict access to only authorized personnel. Personal dosimetry should be worn. It serves as a buffer zone/transition area between the high and low radiation zones. People within this zone at the time of the explosion should be surveyed for contamination before being released	5 - 12 Hrs
1000	High Radiation Zone 1000 - 10000	Restrict access to authorized personnel with specific critical tasks such as firefighting, medical assistance, rescue, extrication, and other time- sensitive activities. Personal dosimetry should be worn. People within this zone at the time of the explosion should be surveyed for contamination before being released.	30 minutes - 5 Hours
10000	Extreme Caution Zone > 10000	This area, located within the high radiation zone, is restricted to the most critical activities, such as lifesaving. Personal dosimetry required. Limit time spent in this area to avoid Acute Radiation Sickness. People within this zone at the time of the explosion must be surveyed for contamination before being released.	Minutes to a few hours

TABLE 1 Possible radiation zones and suggested activities during the first 12 hours
Source: [8] with modifications

As radioactive material spreads, it becomes less concentrated and less harmful. Prompt detection of the type of radioactive material used will greatly assist local authorities in advising the community on protective measures. Radiation and contamination can be readily detected with the suitable equipment. Nevertheless the subsequent decontamination of the affected area may involve considerable time and expense, and requires expert staff. Immediate health effects from exposure to the low radiation levels expected from an RDD would likely be minimal. The deterministic health effects of ionizing radiation are directly proportional to the dose.

In other words, the higher the radiation dose, the higher the risk of injury. This kind of effect is evident only after a specific dose threshold. Early effects occur only to the individuals that receive an effective dose higher than 500 mSv. Late effects, like cancer, could occur also at low dose levels. Yet, just because a person is near a radioactive source for a short time or gets a small amount of radioactive dust on himself or herself this does not mean he or she will get cancer. Exposure at the low radiation doses expected from an RDD would increase the risk of cancer only slightly over naturally occurring rates. Long-term health studies on the survivors of the 1945 nuclear bombings of Hiroshima and Nagasaki indicate that for those who received radiation doses from 0 up to 100 mSv, less than 0.1% of cancers in that population were attributable to radiation [9].

The psychological impact, due to the fear of being exposed, is estimated to be by far the highest source of safety issue in the population after an RDD event. Unless information about potential exposure is made available from a credible source, people unsure about their exposure might seek advice from medical centers, complicating the centers' ability to deal with acute injuries.

Doses and tissue reactions

Symptoms/ Effects	Effective dose threshold [Sv]
No symptoms of illness	< 0.20
No symptoms of illness; minor, temporary decreases in white cells and platelets	< 0.50
No general symptoms of illness; local skin reaction; decreases in white cells and platelets	> 0.50
Possible acute radiation syndrome; 10% will have nausea and vomiting within 48 hours and mildly depressed blood counts	> 1.00
Half of those exposed will die within 30 days without medical care	> 3.00

Conclusions

The safety impact of a radiological device, also in a crowded place, would probably be relatively low, but the uncertainty in the prediction process is really large and it is not easy to be prepared to respond to this kind of event.

The ENEA agency has the required competencies in the radiological field, particularly in radiation protection, and owns the essential hardware and software instruments to face an RDD impact. National and international studies, and experiences developed by ENEA professionals are the basis on which the Agency would construct a complete program for preparing and responding to an event of diffusion of radioactive materials. The main points to be considered are decision-making on protection strategies, public health, monitoring and assessment capability, safety and security of populations and infrastructure, and planning for recovery.

Sandro Sandri
ENEA, Radiation Protection Institute - Radiation Protection for Nuclear Fusion Plants
and Large Accelerators Laboratory

references & notes

[1] ICRP The 2007 Recommendations of the International Commission on Radiological Protection, Publication 103.
[2] J. Preston, 2011, "Radiation Effects", ICRP, www.icrp.org/docs/
[3] World Health Organization, www.who.int/mediacentre/factsheets/fs371/en/
[4] S. Sandri et al, 2008, "Metodi e codici calcolo utilizzati per la valutazione di rilasci in atmosfera di sostanze radioattive volatili", in Atti AIRP 2008 - Convegno Nazionale di Radioprotezione - Pisa 2008.
[5] narac.llnl.gov/HotSpot/
[6] www.oecd-nea.org/tools/abstract/detail/ccc-0553
[7] www.oecd-nea.org/rp/inex/
[8] RDD Handbook: Handbook for Responding to a Radiological Dispersal Device First Responder's Guide–The First 12 Hours, CRCPD, September 2006.
[9] www.rerf.jp/index_e.html

Le nuove frontiere della safety e della security: eventi chimici, biologici, radiologici, nucleari ed esplosivi

La crisi mondiale legata alla riduzione di risorse energetiche fossili, la riduzione di fonti di acqua potabile e la Guerra per il controllo delle fonti di energia rappresentano una parte delle cause che possono condurre ad un evento CBRNe (Chemical, Biological, Radiological, Nuclear, and explosive) di matrice intenzionale. Questo tipo di eventi potrebbe anche essere conseguenza del rilascio accidentale di sostanze (ad esempio, l'incidente di un camion contenente una sostanza chimica industriale tossica) o di eventi naturali, quali uno tsunami o un terremoto. Pertanto, l'elevata percentuale di rischio connesso a un tale accadimento è evidente. Il modo più opportuno di affrontare questo tipo di emergenze è di creare una squadra di Advisors e First Responders CBRNe altamente preparati a supporto dei vertici decisionali, che siano in grado non solo di gestire il rilascio delle sostanze, ma soprattutto di far fronte tempestivamente, e nel medio e lungo termine, alle conseguenze sul territorio colpito dall'evento. Attualmente, gli esperti in materia sono pochissimi e tipicamente concentrati in enti amministrativi centrali. Con il presente articolo, gli autori hanno inteso illustrare le criticità di questo tipo di eventi e le principali conseguenze sociali degli stessi.

New frontiers of safety and security: Chemical, Biological, Radiological, Nuclear, explosive events

The global crisis related to the reduction of energy fossil resources, the reduction of potable water resources and the war for the control of energy sources are part of the causes which can lead to an intentional CBRNe (Chemical, Biological, Radiological, Nuclear, and explosive) event. These kind of events could also be the consequence of an unintentional release of substances (i.e., an accident of a truck containing a Toxic Industrial Chemical), or of natural events like a tsunami or an earthquake. Thus the high percentage of risk connected to their occurrence is clear. The proper way to face these emergencies is to build a team of highly prepared Tech Advisors and First Responders to support Top Decision Makers, not only to deal with the agents released, but mainly to manage the consequences on the territory of occurrence, immediately and in the medium and long term. At the present moment, experts of the kind are really few and usually concentrated in the central administrative bodies. The authors in this work present the criticalities of these kinds of events and their principal societal implications.

DOI: 10.12910/EAI2014-99

■ *A. Malizia, V. Cusmai, V. Rossi, T. Labriola, E. Farrugia, F. Campopiano, F. Salerno, V. Trombadore, L. Cadoni, G. Rezza, R. Fantoni, S. Sandri, M. Chiappini, A. Gucciardino, F. D'Amico, C. Russo, D. Rothbacher, M. Carestia, D. Di Giovanni, O. Cenciarelli, C. Perrimezzi, I. Palombi, C. Bellecci, P. Gaudio*

■ **Contact person: Andrea Malizia**
malizia@ing.uniroma2.it

Introduction

The evolution and proliferation of safety and security issues in the National and International framework made it necessary to respond in a competent and professional way to any crisis scenarios resulting from non-conventional events (i.e., CBRNe events). In all industrialized countries there are Institutions and Facilities with highly specialized groups facing up to emergencies (first responders), but only a few persons are sufficiently trained to manage these incidents. The complexity of these events requires experts not only with a vertical but also with a horizontal knowledge. It is important to understand how extensive is the range of events that can be considered as a CBRNe event, and how different are the answers and implications in the countries all around the world.

The threat today: From toxic industrial chemicals and materials to CBRNe

A CBRNe emergency has not to be intended exclusively as a war or terroristic event, but also as deriving from an unintentional or natural one.

In this section the authors describe some events that can be classified as Chemical or Biological or Radiological or Nuclear or explosive. It is important to point out that the events described below have no connection to one another in terms of emergency planning or intrinsic threat or experts (and actors) involved or rescue methodologies to help the population. Purpose of this section is to give an important message to the readers: many events can be classified as CBRNe and many causes can provoke a CBRNe event. The dispersion of CBRNe materials can be a consequence of:

- natural events (volcanos/earthquakes; storms/inundations; hydrogeological disasters; floods/lack of water; epidemic/pestilences, etc.), or
- accidental events (fires, incidents, etc.)
- events like migration flux or man-made events (i.e., war or terrorism). [13]

The real challenge is getting not only a better knowledge on risks, agents, protection-decontamination and investigation techniques, but also the establishment of a doctrine on prevention capabilities (referred to new NON-Proliferation methodologies), and learning to face non-conventional events and to manage their very consequences.

From a chemical point of view, one of the most well-known unintentional events was the one occurred in 1976 in Seveso, Italy, where a dense vapor cloud was released from a chemical plant manufacturing pesticides and herbicides. In Europe, the Seveso accident prompted the adoption of legislation aimed at the prevention and control of such accidents. The toxic cloud contained tetrachlorodibenzoparadioxin

FIGURE 1 Seveso Disaster

Source: http://unitaecarismi.cittanuova.it/contenuto.php?TipoContenuto=web&idContenuto=35315

FIGURE 2 Viareggio Accident

Source: http://it.wikipedia.org/wiki/Incidente_ferroviario_di_Viareggio#mediaviewer/File:2009_Viareggio_train_explosion_fire.jpg

(TCDD), a by-product of the trichlorophenol synthesis, also known as Seveso dioxin. TCDD has poisonous and carcinogenic properties with an LD50 of 0.02 mg/kg. Although no fatalities were reported, soon after its release a large amount of different toxic chemicals were dispersed in the environment and spread on a large area. This resulted in the immediate contamination of some ten square miles of land and vegetation. More than 600 people had to be evacuated from their housings and as many as 2000 were treated for dioxin poisoning [1] (Fig. 1).

Moving to recent years, another chemical, accident-related event is the one occurred in Viareggio, Italy, in 2009 (Fig. 2).

The Viareggio derailment of a freight train and subsequent fire occurred on June 29, 2009, in a railway station in Viareggio, (province of Lucca), a city in Central Italy's Tuscany region.

Some of the wagons were reported to have been carrying Liquefied Petroleum Gas (LPG). Two of these exploded and caught fire. Seven people were reported to have died in a building collapse.

Among the unintentional biological events, the 2009 swine flu A-H1N1 pandemic can be considered as a blatant example of biological threat. The disease originated from a mutation occurred in a swine flu virus, that acquired the ability to infect humans and, subsequently, to be contagious from human to human (Fig. 3). In 2009, the A-H1N1 flu pandemic spread fast worldwide, causing several hundreds of deaths and thousands of contagions, especially in America. The World Health Organization and the Centers for Disease Control and Prevention considered it as pandemic due to its global diffusion. Since then, people continued to get sick from swine flu, but not so frequently as before [2]. On October 24, 2009, the US President signed a statement declaring the 2009 A-H1N1 pandemic flu as a national emergency. It enabled to respond to the pandemic by allowing – if warranted – the waiver of certain statutory Federal requirements for medical treatment facilities. [3]

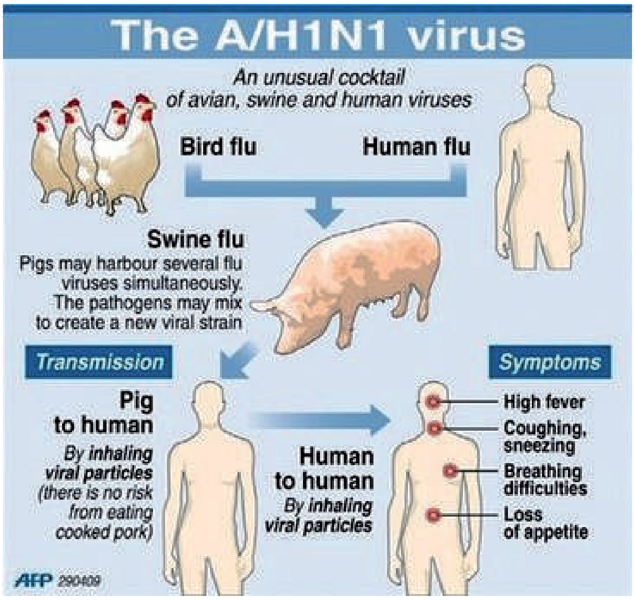


FIGURE 3 H1N1 a contemporary pandemic
Source: http://dxline.info/diseases/h1n1-influenza

FIGURE 4 Tsunami at Fukushima
Source: http://www.corriere.it/gallery/esteri/05-2011/tepco/1/tsunami-investe-fukushima_52bd44c4-81ec-11e0-817d-481efd73d610.shtml#

The last (but not least) accidental event, in this case from a radiological point of view, is the one that perhaps impressed us the most, but negatively: the Fukushima Daiichi nuclear disaster, a catastrophic failure at the Fukushima I Nuclear Power Plant on March 11, 2011. The failure occurred after the tsunami triggered by the Tōhoku earthquake hit the nuclear plant (Fig. 4) and substantial amounts of radioactive materials were released starting on March 12. This has become the largest nuclear incident since the 1986 Chernobyl disaster, and the second (with Chernobyl) to measure Level 7 on the International Nuclear Event Scale

(INES). 300,000 people had to be evacuated from the area, approximately 18,500 died in the earthquake and tsunami events, and, as in August 2013, approximately 1,600 deaths were attributed to the evacuation conditions, such as living in temporary housing and hospital closures. [4]

These are just four of the most well-known examples of disasters that can be listed as CBRNe events of unintentional or natural origin. Thousands of natural events involve dispersion of chemical, biological or radiological materials (i.e., earthquakes, hurricanes, tsunami, and natural epidemics). It is clear that the victims are related to the fact the radioactive contamination levels for humans are too high.

Frequently people link CBRNe threats to war or terrorism scenarios. Below few examples of CBRNe events in the contexts of war or terrorism are reported.

One of the most famous intentional events linked to Chemical Weapons (CW) is the first use of Mustard Gas during the First World War when, in 1917, the German army fired artillery shells against British and Canadian soldiers near Ypres, Belgium. The place where the chemical agent was used for the first time gave the name to the aggressive chemical today still known as Yperite. Delivered by artillery shells, Mustard Gas caused more than 20,000 casualties and remained active for weeks because of its persistency in the environment. This represented a problem since the contaminated areas remained unusable for long periods. The protection devices available against Mustard Gas were relatively ineffective: although the mask filters partially protected the lungs from the inhalation contamination, no shield was offered to the blister effects due to the contact between the chemical warfare agent and the skin [5] (Fig. 5).

FIGURE 5 Soldiers at Ypres during the WWI
Source: http://www.thehistorypostblog.co.uk/tag/mustard-gas/

FIGURE 6 Nuclear explosion
Source: http://www.planetdeadly.com/human/incredible-nuclear-explosion-photos

Biological Weapons (BW) were never extensively used in war even if, especially during the two World Wars, some countries started a program of biological weapons. One of the most notorious research program focused on the weaponization of biological agents and the development of biological weapons was conducted during World War II by the secret Imperial Japanese Army Unit 731, based at Pingfan (Manchuria) and commanded by Lieutenant General Shirō Ishii. In this unit fatal experiments on prisoners were conducted: microorganisms were inoculated in order to study the pathogenesis and the virulence of the inducted diseases, and dissections were done without anesthesia. Although the Japanese effort lacked of the technological sophistication of the American or British programs, it far outstripped them in its widespread application and indiscriminate brutality. Biological weapons were used against both Chinese soldiers and civilians in several military campaigns. In 1940, the Imperial Japanese Army Air Force bombed Ningbo with ceramic bombs full of fleas carrying the plague.

Many of these operations were ineffective due to inefficient delivery systems, although up to 400,000 people may have died [6]. Attacking animals is another area of biological warfare intended to eliminate animal resources for transportation and food. During the First World War, German agents were arrested while attempting to inoculate draught animals with anthrax, and they were believed to be responsible for outbreaks of glanders in horses and mules.

It is easy to associate a nuclear event to war: Hiroshima and Nagasaki are two unforgettable shocking moments of our contemporary history. The atomic bombings of the cities of Hiroshima and Nagasaki in Japan were conducted by the United States during the final stages of World War II in 1945. The two events are the only use of nuclear weapons in war to date. The Little Boy atomic bomb was dropped on the city of Hiroshima on August 6, 1945, followed by the Fat Man bomb on the city of Nagasaki on August 9. Within the first two to four months of the bombings, the acute effects killed 90,000–166,000 people in Hiroshima and 60,000–80,000 in Nagasaki, with roughly half of the deaths in each city occurring on the first day. During the following months, large numbers died from the effect of burns, radiation sickness and other injuries, compounded by illness. In both cities, most of the dead were civilians, although Hiroshima had a sizeable garrison [7] (Fig. 6).

Finally, to give a more general description of the international scenario, it is necessary to describe some CBRNe events related to terrorism.

Starting from chemical events, the most famous event is the Sarin gas release in Tokyo's subway on March 20, 1995. Five members of the Aum Shinrikyo cult launched a chemical attack in Tokyo's subway, one of the world's busiest commuter transport systems, at the peak of the morning rush hour. Sarin, the chemical agent which was released, was contained in plastic bags wrapped in newspaper. Each perpetrator carried two packets totalling approximately 900 milliliters of sarin, except Yasuo Hayashi, who carried three bags. Aum originally planned to spread the Sarin as an aerosol but did not follow through with it. Carrying their packets of Sarin and umbrellas with sharpened tips, the perpetrators boarded their appointed trains. At prearranged stations, the Sarin packets were dropped and punctured several times with the sharpened tips of the umbrella. Each perpetrator then got off the train and exited the station to meet his accomplice with a car. By leaving the punctured packets on the floor, Sarin, which is a very volatile substance, was allowed to leak out into the train and stations. This chemical agent affected passengers, subway workers, and those who came into contact with them [8] (Fig. 7).

FIGURE 7 Sarin attack in Tokyo
Source: http://matome.naver.jp/odai/2136380668192730201

FIGURE 8 Letters with B contamination
Source: http://qn.quotidiano.net/cronaca/2012/12/04/812127-pacco-sospetto-antrace-ricoverati-ospedale.shtml

A terrorist use of biological agents is represented by the well-known 2001 anthrax attacks in the United States, also called Amerithrax by the Federal Bureau of Investigation (FBI). The attacks occurred over the course of several weeks, beginning one week after the September 11 attacks. The first set of anthrax letters had a Trenton, New Jersey postmark dated September 18, 2001. Five letters are believed to have been sent at that time to: ABC News, CBS News, NBC News and the New York Post, all located in New York City, and to the National Enquirer at American Media, Inc. (AMI) in Boca Raton, Florida. A series of conflicting news reports appeared, some of them claiming that the powders had been weaponized with silica. Bioweapons experts, who later viewed images of the anthrax attacks, saw no indication of weaponization and tests by Sandia National Laboratories in early 2002 confirmed that the attack powders were not weaponized. At least 22 people developed anthrax infections, 11 of these with the especially life-threatening inhalational variety [9] (Fig. 8).

Speaking about R-N terrorist attack, one of the most known was the Alexander Litvinenko (Fig. 9) murder. In UK, Litvinenko became a journalist for a Chechen separatist site. On November 1, 2006, Litvinenko suddenly fell ill and was hospitalized. For several days he suffered of severe diarrhea and vomiting. At one point, he could not walk without assistance.

For several weeks, Litvinenko's health conditions worsened and doctors began to investigate the causes of his illness. Litvinenko became physically weak, and spent periods unconscious. He died three weeks later, becoming the first confirmed victim of lethal Polonium-210-induced acute radiation syndrome. According to the doctors, "Litvinenko's murder represents an ominous landmark: the beginning of an era of nuclear terrorism" [10].

FIGURE 9 Litvinenko

Source: http://www.repubblica.it/2006/12/sezioni/esteri/spia-avvelenata-3/litvinenko-bersaglio/litvinenko-bersaglio.html

War, terrorism but also explosions, accidents and natural disasters can provoke CBRNe events, attempting the safety of people and operators and the security of environments and structures. CBRNe risk is a concrete threat and new scenarios are opening in this field.

It is difficult to place events like the dispersion of chemical substances in Iraq and in Syria in one specific category. Are these events War? Terrorism? The new frontiers of risks have unknown and unexpected characteristics.

Different mentality with a common enemy

The loss of national control and the global spread of knowledge related to chemical, biological, radiological and nuclear weapons and technologies have been a long-standing concern in the post-Cold War World. In recent years, the fear that terrorist groups might employ CBRNe agents has particularly increased as some of these sensitive technologies and under pinning scientific knowledge have become more easily available for use in crude weapons. The National Security Strategy places a strong emphasis on these concerns by including the risk of international terrorism activity with the possibility of using CBRNe agents at the highest priority level; the risk of CBRNe attacks from state actors ranks just one priority level below. Multidisciplinary research, focused on the long-term perspective, will play an important role in understanding the implications of constant rapid technological development in the CBRNe area. It will also allow enlightening how the global spread of scientific education might affect aspirations of different State and non-State actors to use these technologies and knowledge for malevolent actions. A clearer understanding of these developments and the direction they may take will aid the progress of more effective policies and tools to counter possible CBRNe threats [11].

Because of security budget reduction, the way in which different Countries prepare for CBRNe incidents deserves renewed attention; this involves the prioritization of capabilities against C, B, R, or N in the Analysis, Prevention and Response (APR) phases. It will also be necessary to acquire detailed information about the capability of the actor involved to use or produce CBRNe weapons, taking into account all the latest scientific developments in the field of chemistry, physics, biology and nanotechnology. An analysis of how actual CBRNe threats and hazards are perceived by policy makers from different Countries shows the following outcomes:

- there is a consensus on the importance of CBRNe threats. Some Countries list CBRNe-terrorism, or CBRNe-weapon use and proliferation among the most important security threats;
- the general perception is that State actors have the potential to acquire CBRNe expertise and experts, but are restrained to deploy them; the opposite holds to be true for non-State actors.

With respect to science and technology, experts expect: (a) an increasing interaction between chemistry and biology know-how development; (b) dramatic advances in understanding and manipulating genes, cells, and organisms, and (c) developments in the field of nanotechnology that may revolutionize dispersal methods. With respect to materials: (a) an increasing availability of CBRNe materials; (b) the potential to engineer (CB) materials from scratch and (c) a growth in the number of dual-use materials and technology that pose major challenges to non-proliferation regimes. With respect to intentions: (a) a persistent intention on the part of State actors to acquire new types of CBRNe capabilities and (b) a persistent intention on the part of non-State actors to acquire new types of CBRNe capabilities and in some cases an explicit desire to use these capabilities. Overall, experts agree that in the 21st century CBRNe agents may be used and deployed as weapons in novel ways, both in the military and civil domains. This reveals how countries formulate and execute their respective CBRNe policies. The conclusion is that some countries deal with CBRNe as a single policy issue in its own right; other countries approach CBRNe as part of a larger security policy approach; CBRNe crisis management has shifted from the military to the civil domain resulting in a duplication of efforts. While capabilities have been strategically identified along the APR phases, few countries have developed specific CBRNe strategies [12].

Conclusions

The CBRNe world offers several starting points for national and international collaborations in a wide range of public, private, research, and industrial contexts. It is important to create the conditions to connect the best experts, allowing a reverse brain-drain process. Why pursuing this challenge? To create a new way of working together and, above all, to have a new vision of work. It is essential to identify the needs in the CBRNe safety and security framework and then deploy existing skills and develop new theoretical and practical knowledge to answer those needs. The problems presented in this paper give just an overview of a more complex scenario. It is necessary have well-prepared experts to face these particular events. The Department of Industrial Engineering and the School of Medicine and Surgery of Rome's University of Tor Vergata decided to face these problems with the "International Master Courses in Protection Against CBRNe events" presented in the paper: "Building a CBRNe Tech Advisor and First Responders Team to support Top Decision Makers during the emergencies" printed in this issue of EAI-ENEA.

Acknowledgements

Special Acknowledgments to the International Master Courses in Protection Against CBRNe events. Further information available at: www.mastercbrn.com. Enrollment for A.Y. 2014/2015 OPEN.

Andrea Malizia, Fabrizio D'Amico, Dieter Rothbacher, Mariachiara Carestia, Daniele Di Giovanni, Orlando Cenciarelli, Carlo Bellecci, Pasqualino Gaudio
University of Rome Tor Vergata, Industrial Engineering Department

Vittorio Cusmai
Italian Defence Staff, Division I

Vincenzo Rossi
Italian Ministry of the Interior

Tiziano Labriola
Italian Presidency of the Council of Ministers

Emanuele Farrugia
Italian Ministry for Foreign Affairs

Francesco Campopiano
Italian Presidency of the Council of Ministers, Civil Protection Dept.

Franco Salerno
Joint NBC Defence School

Vincenzo Trombadore
Italian Ministry of the Interior, Public Security Dept.

Luciano Cadoni
Italian Ministry of the Interior, Firefighters Dept.

Giovanni Rezza
ISS - Istituto Superiore di Sanità (Italian National Institute of Health)

Roberta Fantoni
ENEA, Technical Unit for the Development of Applications of Radiation

Sandro Sandri
ENEA, Radiation Protection Institute - Radiation Protection for Nuclear Fusion Plants and Large Accelerators Laboratory

Massimo Chiappini
Istituto Nazionale di Geofisica e Vulcanologia (INGV)

Antonio Gucciardino
University of Tor Vergata, Scientific Board of International Master Courses in Protection Against CBRNe events, Department of Industrial Engineering and School of Medicine and Surgery

Colomba Russo, Carlo Perrimezzi
Crati Scrl - Consorzio per la ricerca e le applicazioni di tecnologie innovative

Leonardo Palombi
University of Rome Tor Vergata, School of Medicine and Surgery - Department of Biomedicine and Prevention

references & notes

[1] http://ec.europa.eu/environment/seveso/
[2] http://www.webmd.com/cold-and-flu/flu-guide/h1n1-flu-virus-swine-flu
[3] http://www.flu.gov/planningpreparedness/federal/h1n1emergency10242009.html
[4] http://en.wikipedia.org/wiki/Fukushima_Daiichi_nuclear_disaster
[5] http://en.wikipedia.org/wiki/Sulfur_mustard#History
[6] http://en.wikipedia.org/wiki/Biological_warfare#Interwar_period_and_WWII
[7] http://en.wikipedia.org/wiki/Atomic_bombings_of_Hiroshima_and_Nagasaki
[8] http://en.wikipedia.org/wiki/Sarin_gas_attack_on_the_Tokyo_subway
[9] http://en.wikipedia.org/wiki/2001_anthrax_attacks
[10] http://en.wikipedia.org/wiki/Poisoning_of_Alexander_Litvinenko
[11] http://www.globaluncertainties.org.uk/research/weapons-proliferation/
[12] http://www.hcss.nl/reports/navigating-the-cbrn-landscape-of-2010-and-beyond-towards-a-new-policy-paradigm/15/
[13] R. Fiorito, C. Bellecci, A. Gucciardino, A. Malizia, F. D'Amico, C. Fontana, C. Russo, C. Perrimezzi, P. Gaudio, 2013, "Training internazionale: eventi accidentali, naturali, dolosi = EVENTI CBRNe", in AIRP - Atti del XXXVI Convegno Nazionale di Radioprotezione, Palermo, 18-20 settembre 2013, V sessione, BOLLETTINO AIRP, p. 61-69, ISBN 978-88-88648-38-5, ISSN 1591-3481.

La dimensione umana della security e i Centri di Eccellenza

La dimensione umana, che abbraccia la cultura della security e dello sviluppo delle risorse umane, è alla base di un regime di security nucleare o CBRN (chimico, biologico, radiologico e nucleare). Diversi Paesi hanno inaugurato o stanno pianificando centri nazionali o Centri di Eccellenza di formazione e supporto per la security nucleare (o CBRN). Diverse iniziative a livello regionale sono in corso, delle quali la CBRN Centres of Excellence Initiative dell'Unione Europea è la più importante. A livello internazionale, l'IAEA (International Atomic Energy Agency) ha assunto un ruolo di coordinamento attraverso l'International Network for Nuclear Security Training and Support Centres. Nel quadro del Nuclear Security Summit, l'Italia ha presentato un Gift Basket che promuove il networking e la cooperazione internazionale tra i centri per la security.

Developing the human dimension of security by means of Centres of Excellence

The human dimension, encompassing the culture of security and human resources development, is the foundation of a sustainable nuclear – or chemical, biological, radiological and nuclear (CBRN) – security regime. Several countries have established, or are planning to establish, national nuclear (or CBRN) security centres, or Centres of Excellence for training and support. Initiatives at the regional level are also under way, of which the EU CBRN Centres of Excellence Initiative is the most important. At the international level, the IAEA (International Atomic Energy Agency) is assuming a coordinator role through the International Network for Nuclear Security Training and Support Centres. In the Nuclear Security Summit framework, Italy introduced a Gift Basket promoting networking and international cooperation among security centres.

DOI: 10.12910/EAI2014-100

■ *F. Padoani, A. Rizzo*

Introduction

The human dimension is the key element underpinning nuclear security and, more in general, CBRN security. The origin of any security event, whether malicious or not, can ultimately be tracked down to the human factor. Security culture and human resource development are essential components of an effective security regime and its sustainability.

The Nuclear Security Summit (NSS) process [1] has played an important role in fostering the importance of the human dimension. The 2010 Washington NSS gave it an unprecedented importance for a high-level political event; then the 2012 Seoul NSS further recognized the fundamental importance of investing in

■ **Contact person: Franca Padoani**
franca.padoani@enea.it

human capacity-building for promoting and sustaining a strong nuclear security culture, while encouraging States to promote human resource development through education and training.

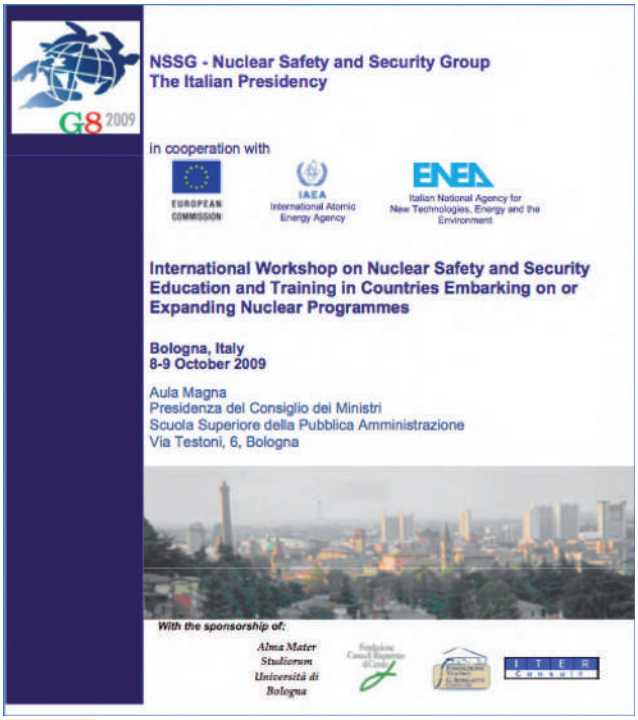
Several countries have established in recent years, or are planning to establish, national nuclear (or CBRN) security centres. Initiatives at the regional level are also under way, strengthening a regional culture of security in a synergic manner: the European Union's Chemical, Biological, Radiological and Nuclear Centres of Excellence (EU CBRN CoE) Initiative is the most relevant example in this field. At the international level, the IAEA is assuming a coordinator role with respect to nuclear security through the International Network for Nuclear Security Training and Support Centres (NSSC Network).

The Italian contribution

From the Italian G8 Presidency in 2009 to the Nuclear Security Summits

Italy has been paying special attention to education, training and institutional capacity building as essential elements to an effective safety and security infrastructure since the Italian G8 Presidency in 2009. In the framework of the G8 Nuclear Safety and Security Group, Italy organized an International Workshop on Nuclear Safety and Security Education and Training in Countries Embarking on or Expanding Nuclear Programmes, with the support of the IAEA, the European Commission and ENEA, in Bologna in October 2009 (see Fig. 1). The recommendations of this Workshop now constitute important elements of the Washington NSS Communiqué and Work Plan and are now being implemented worldwide.

Following on from this, at the Washington Summit in 2010 Italy announced the creation of an International School on Nuclear Security with the IAEA and the International Centre for Theoretical Physics (ICTP) in Trieste. The School held its fourth two-week course in May 2014, a successful initiative much appreciated by the participants and widely recognized by the international community. Many of the participants were from developing and emerging countries, mainly from Asia and Africa, and from regulatory bodies, universities, research institutes, government ministries and law enforcement agencies.



G8 2009

NSSG - Nuclear Safety and Security Group
The Italian Presidency

in cooperation with

EUROPEAN COMMISSION

IAEA
International Atomic Energy Agency

ENEA
Italian National Agency for New Technologies, Energy and the Environment

International Workshop on Nuclear Safety and Security Education and Training in Countries Embarking on or Expanding Nuclear Programmes

Bologna, Italy
8-9 October 2009

Aula Magna
Presidenza del Consiglio dei Ministri
Scuola Superiore della Pubblica Amministrazione
Via Testoni, 6, Bologna

With the sponsorship of:

Alma Mater Studiorum Università di Bologna

ITER Consult

FIGURE 1 The G8 International Workshop in Bologna, 2009

The NSSC/CoE Gift Basket

Although under different names such as training centres, schools or centres of excellence, in recent years many centres have been or are in the process of being set up, at the national, regional or international levels. With the network rapidly expanding, a coordination effort is essential in order not only to prevent overlapping but also to enhance the leveraging of resources, particularly at the regional level. The IAEA effort towards this end, finally leading to the creation of the NSSC Network, is therefore commendable, as are European efforts at the regional level with the CBRN CoE Initiative.

An awareness of these issues led to Italy's decision to sponsor the Nuclear Security Training and Support Centres / Centres of Excellence (NSSC/CoE) Gift Basket at the Nuclear Security Summit in The Hague, in 2014 [1]. The Gift Basket recognizes the expansion of the

Joint statement on Nuclear Security Training and Support Centres / Centres of Excellence for the 2014 Nuclear Security Summit submitted by Italy

On the occasion of the 2014 The Hague Nuclear Security Summit, the following States, Algeria, Argentina, Armenia, Australia, Belgium, Canada, Chile, France, Georgia, Germany, Hungary, Indonesia, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Lithuania, Mexico, Morocco, the Netherlands, Pakistan, Philippines, Romania, Spain, Sweden, Turkey, United Arab Emirates, the United Kingdom, the United States and Vietnam recall the Joint Statement on Nuclear Security Training and Support Centres (NSSCs) issued at the 2012 Summit held in Seoul, Republic of Korea, and note that the International NSSC Network now has over 100 members from 39 States and that 12 States have established such centres since the 2010 Nuclear Security Summit.

The States noted above reaffirm the value of the NSSC Network in strengthening international and regional cooperation and collaboration to promote nuclear security education and training. They also encourage the IAEA and other stakeholders to work with and to support the further development of nuclear security training and support centres / centres of excellence and to explore the synergies between education and training that such centres can provide for national, regional and global nuclear security.

They welcome the IAEA's activities carried out in conjunction with the NSSC Network to promote the establishment of centres and, in particular, activities to provide for the exchange of information and best practice that would strengthen capacity building and nuclear security culture, and maintain a well-trained cadre of technical experts in States.

Acknowledging the importance of the NSSC Network to promote coordination amongst such centres and recognising the importance of avoiding duplication and overlap, they also encourage regional cooperation initiatives and other initiatives to facilitate greater information sharing on and harmonization of respective capabilities and plans among individual centres in particular regions.

Joint Statement on Nuclear Security Training and Support Centres resulting from the 2012 Seoul NSS

On the occasion of their participation in the 2012 Seoul Nuclear Security Summit, Algeria, Australia, Canada, Chile, Czech Republic, Germany, Hungary, Indonesia, Italy, Japan, Jordan, Kazakhstan, Republic of Korea, Lithuania, Malaysia, Mexico, Morocco, Netherlands, Pakistan, Philippines, Ukraine, United Arab Emirates, the United Kingdom, and the United States note their intent to collaborate in the form of the International Network for Nuclear Security Training and Support Centres (NSSCs) aiming to build up a cadre of highly qualified and well trained nuclear security personnel, provide specific technical support required for effective use and maintenance of instruments and other nuclear security technical systems, as well as provide scientific support for the detection of and the response to nuclear security events in a country.

In accordance with its Nuclear Security Plan for 2010-13 approved by the Board of Governors in September 2009, the International Atomic Energy Agency's Office of Nuclear Security supports these member states through coordination of the activities of the Network. The IAEA's Nuclear Security Web Portal (NUSEC) provides a platform to facilitate coordination and sharing of best practices. These NSSCs enhance nuclear security at the national level and promote many of the elements of the Communiqué and Work Plan of the 2010 Washington Nuclear Security Summit and the Communiqué of the 2012 Seoul Nuclear Security Summit. In particular, they support human resource development and education and training in nuclear security, enhance nuclear security culture, and maintain a well-trained cadre of technical experts.

BOX 1 Gift Basket (or Joint Statement) on Nuclear Security Training and Support Centres / Centres of Excellence (NSSC/CoE) presented by Italy at the Nuclear Security Summit in The Hague

network, while further promoting the development of nuclear security training and support centres/centres of excellence, in this way encouraging networking and international and regional cooperation. ENEA has been designated as the reference institution, acting as Scientific Secretariat for the Gift basket.
The text of the Gift Basket is shown in Box 1.

The NSSC Network

The Network for Nuclear Security Training and Support Centres (NSSC Network) was established in February 2012 with the IAEA in a coordinator role and serving as secretariat. The NSSC Network objectives are on the one hand to promote a high level of nuclear security training and support services and, on the other hand, to facilitate cooperation and assistance (also technical and scientific) and to optimize the use of available resources.
The NSSC Network centres, although under different names (NSSC, CoE, and so on), all have the shared aim of developing human resources in nuclear security, enhancing nuclear security culture, and maintaining a well-trained cadre of technical experts. Some Centres have set up regional networks, such as the recent Asian Regional Network (ARN) by South Korea, China and Japan. The EU CBRN CoE Initiative, through its regional approach, is complementary and synergic to the NSSC Network.
Several national centres have been or are being established following the IAEA concept of NSSCs based on three elements: the development of human resources through tailored training programmes; the development of a network of experts; the provision of technical support for equipment during its lifecycle, and scientific support for the detection of and response to nuclear security events (see Fig. 2).
As the number of NSSCs/CoE increases and operational experience is acquired, they may evolve in different ways from the initial concept, in order to better reflect the nation needs. For example some have extended their scope beyond nuclear security to encompass the full CBRN spectrum threat and emergency preparedness and response. In this respect, one interesting example is Kenya which initially established a centre with IAEA support following the NSSC concept and then, also

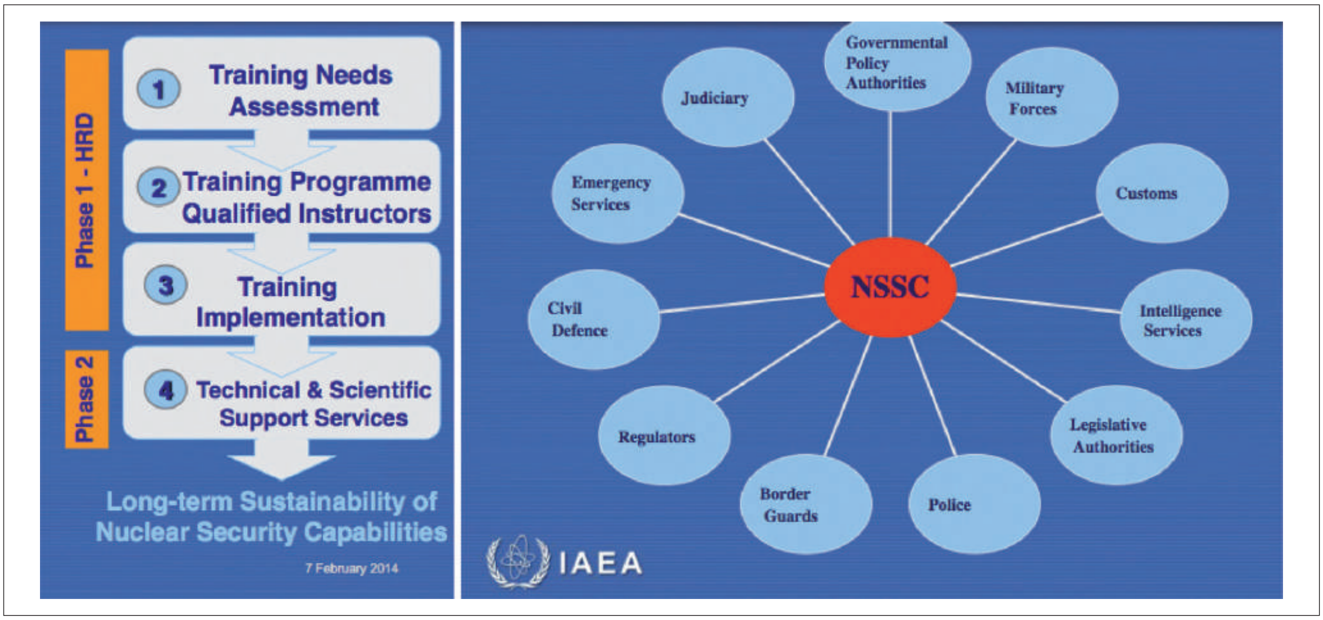


FIGURE 2 The IAEA concept for the establishment of NSSCs
Source: IAEA

thanks to the influence of activities of the EU CBRN CoE Initiative, further developed the structure, changing its name to the Nuclear Security Coordination Centre, in order to deal with the CBRN threat both in the case of malicious acts and of natural catastrophes.

The NSSC Network is closely linked to the INSEN, the International Nuclear Security Education Network [2]: two-way communication exists between the two networks recognizing the mutual advantages of collaboration on a number of common and cross-cutting activities, such as peer review and the preparation of training and educational material.

As of March 2014, the NSSC Network consists of more than 90 members from more than 40 institutions, recognizing the need for coordinated collaboration. The activities are organized in three working groups: WG A – Coordination and Collaboration, WG B – Best Practices, and WG C – Information Management and Other Emerging Issues. The annual meeting is the major event and the forum for the exchange of information with the other international organizations relevant to the NSSC/CoE development. One of the most important ones in addition to the EU with its CBRN CoE initiative is the G8 Global Partnership subgroup on Centres of Excellence.

The EU CBRN CoE initiative

The EU CBRN Risk Mitigation – Centres of Excellence (CBRN CoE) initiative was launched in 2010 by the European Union, as an instrument to bring together the activities relating to the mitigation of CBRN risks in countries outside Europe, addressing the gaps in coordination and fragmentation at the national level, and promoting the sharing of good practices and expertise between European and non-European countries.

The CBRN threat

Any malevolent use of chemical, biological, radiological and nuclear agents against persons and the environment, including the agro-food chain, is considered a CBRN threat. However, one of the most important threats comes from the spread of technical knowledge and capabilities that can enable subversive individuals or groups to build CBRN devices: hence, once again, the need for a strong security culture. The level of threat from terrorist attacks depends on the chosen CBRN agent, technical expertise and means of delivery available to terrorist groups.

Particularly in the case of bio and chemical agents, the development of new techniques and new processes

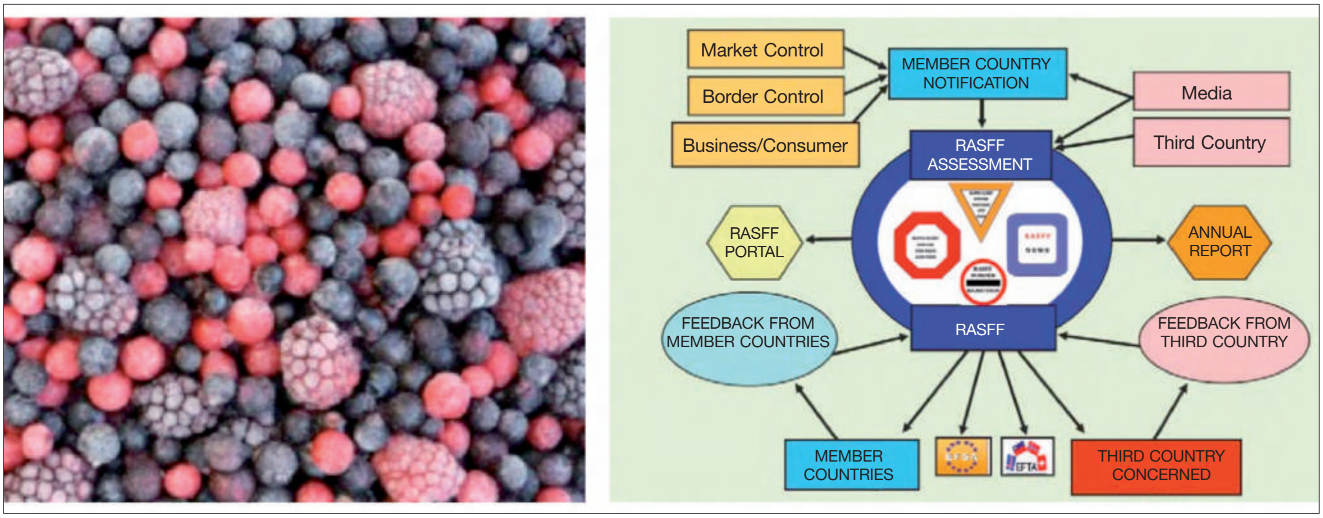


FIGURE 3 Frozen berries in the EU market, found to be contaminated with hepatitis-A in 2014, and the RASFF system for alert on food contamination
Source: 2012 Report http://ec.europa.eu/food/food/rapidalert/docs/rasff_annual_report_2012_en.pdf

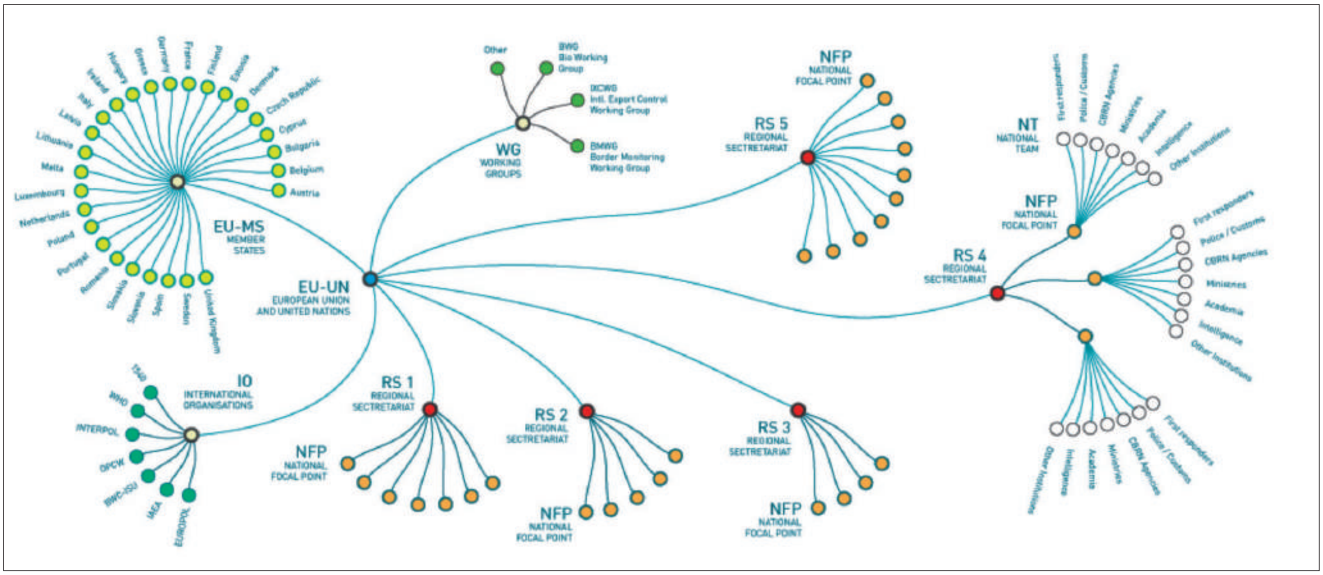


FIGURE 4 The structure of the EU CBRN CoE network
Source: http://www.cbrn-coe.eu/AboutCoE.aspx

(like microfluidics, nanotechnologies and microwave reactors) are resulting in the downscaling of productive systems, facilitating the operation of innovative technology in very small environments, thus increasing the possibility of evading control. Biological agents could also be used to contaminate food, facilities and the agricultural productive chain with a huge potential psychological impact on the population. To address this threat, the EU has implemented the monitoring of chemical and biological risks in the food chain by setting up the RASFF alert system (Rapid Alert System for Food and Feed), http://ec.europa.eu/food/food/rapidalert/index_en.htm (see Fig. 3).

The responsibility to protect civilian populations against CBRN threats is assigned to States and the ultimate barrier is the capacity of the State to prevent, detect and respond to these threats. Each stage – prevention, detection and response – requires specific competences that need to be developed, maintained and sustained by the State. At the European level, the EU is playing a key coordination role in strengthening the CBRN security, and one important tool is the EU CBRN Action Plan aiming to complement national measures in European countries.

The CBRN CoE initiative

Echoing and integrating the CBRN Action Plan, with the Instrument Contributing to Stability and Peace (the successor to the Instrument for Stability from March 2014), the EU launched the EU CBRN Risk Mitigation – Centres of Excellence Initiative [3] in 2010 with the aim of coordinating in a synergic manner all the activities relating to the mitigation of CBRN risks in countries outside Europe, focusing above all on institutional capacity-building.

The structure (see Fig. 4) is based on Regional Secretariats with the role of facilitating coordination and cooperation with the partner countries and the implementation of projects funded through this Initiative in the region. The interaction of the Regional Secretariats with the partner countries takes place through the designated CBRN CoE National Focal Points, the key players of the Initiative at the national level. The role of the National Focal Points is also to set up a National CBRN CoE Team of experts from the bodies and ministries operating in the field of CBRN risk mitigation. The CBRN CoE Regional Secretariats are currently operating in the following eight regions:

Project	Title	Area
040	Strengthening health laboratories to minimize potential biological risks	B
039	Strengthening health security at ports, airports and ground crossings	CBRN
038	Export control outreach for dual use items	CBRN
037	MEDILABSECURE - Establishment of networks of human and animal virology laboratories and of medical entomology	B
036	Further development and consolidation of the Mediterranean Programme for Intervention Epidemiology Training (MediPIET)	B
035	Management of hazardous chemical and biological waste in the African Atlantic Façade region and Tunisia	CB
034	Strengthening capacities in CBRN event response and related medical emergency response under strengthened CBRN event preparedness	CBRN
033	Strengthening the national CBRN legal framework and provision of specialized and technical training to enhance CBRN preparedness and response capabilities	CBRN
032	Establishment of a Mediterranean Programme for Intervention Epidemiology Training (MediPIET)	B
031	Network of universities and institutes for raising awareness on dual-use concerns of chemical materials	C
030	Network of Excellence for Nuclear Forensics in South East Asia Region	N
029	Regional Human Resource Development for Nuclear Safety, Security, and Safeguards Management through a University Master's Programme carried out in Thailand	N
028	Supporting development of an integrated national security system for nuclear and radioactive materials	R
027	Bio-risk management	B
026	Prerequisite to strengthening CBRN national legal frameworks	CBRN
025	Knowledge development and transfer of best practice on bio-safety/bio-security/bio-risk management	B
024	Development of a methodology for RN materials detection, management and protection of the public	R
023	Building capacity to identify and respond to threats from chemical, biological, radiological and nuclear substances	CBRN
022	Provision of specialized technical training to enhance the first responders' capabilities in case of CBRN incidents	CBRN
021	Building regional border control capacity to identify and detect CRN materials	CBRN
019	Development of procedures and guidelines to create and improve secure information management systems and data exchange mechanisms for CBRN materials under regulatory control	CBRN
018	International Network of universities and institutes for raising awareness on dual-use concerns in bio-technology	B
017	Establishing a National Response Plan in Ghana and Kenya for responding to unauthorized events involving chemical, biological, radiological and nuclear (CBRN) materials	CBRN
016	Supporting development of an integrated national nuclear security system	N
015	Strengthening laboratory bio-safety and bio-security through development of a laboratory iso-bank system	B

014	Provision of specialized and technical training to enhance the First Response CAPabilities (CBRN FRstCap)	CBRN
013	Capacity building and raising awareness for identifying and responding to threats from chemical, biological, radiological and nuclear materials in Sub Saharan African countries	CBRN
012	Sharing experience between EU and South East Asian countries on the reinforcement of legislations and regulations in the field of bio-safety and bio-security, as well as relevant laboratories management systems through Regional Centre of Excellence - phase 2	B
011	Promoting good practice and inter-agency procedures for assessing the risks of chemical, biological, radiological and nuclear misuse	CBRN
010	Development of e-learning courses for CBRN risk mitigation	CBRN
009	National Response Plan in Lebanon for CBRN Events	CBRN
008	Prerequisite to strengthening CBRN national legal frameworks	CBRN
007	Guidelines, procedures and standardisation on bio-safety/bio-security	B
006	Knowledge development and transfer of best practice on chemical and biological waste management	CB
005	Knowledge development and transfer of best practice on CBRN import/export monitoring	CBRN
004	Inter-agency CBRN Response Programme (ICP)	CBRN
003	Knowledge development and transfer of best practice on bio-safety/bio-security/bio-risk management	B
002	Building CAPacity to identify and respond to threats from Chemical, Biological, Radiological and Nuclear substances (CBRNcap)	CBRN
001	Identification and strengthening forensic capacities in the area of prevention of organized crime and illicit trafficking of chemical agents, including training and equipment for the line officers	C

TABLE 1 List of EU CBRN CoE initiative projects as of June 2014
Source: http://www.cbrn-coe.eu/

- African Atlantic Façade;
- Central Asia;
- Eastern and Central Africa;
- Gulf Cooperation Council Countries;
- Middle East;
- North Africa;
- South East Asia;
- South East Europe, Southern Caucasus, Moldova and Ukraine.

For the period 2014-2020, the CBRN CoE initiative can count on a budget of €156 million. A total of 40 CBRN CoE Initiative projects had been funded by the EU at the end of 2013. All projects aim at awareness-raising and capacity-building, as shown in Table 1.

ENEA and the CBRN CoE initiative

ENEA has been involved in the Instrument Contributing to Stability and Peace from the very beginning, actively engaged as coordinator or partner in the implementation of projects in the framework of the Expert Support Facilities (ESF) and of the EU CBRN CoE Initiative. Even before the launch of the EU CBRN CoE Initiative, ENEA was coordinator of the project ESF-LOT5 "CBRN Training Centre on Safety and Security", contributing to the definition of the concept of the EU CBRN CoE network. The ESF-LOT3 project on "Redirection of former weapon scientists and engineers" has recently been concluded. ENEA is currently coordinating two ongoing projects of the CBRN CoE Initiative:

- Project 13 “Capacity building and raising awareness for identifying and responding to threats from chemical, biological, radiological and nuclear materials in Sub Saharan African countries”. Geographical scope: Eastern and Central Africa.
- Project 31 “Network of universities and institutes for raising awareness on dual use concerns of chemical materials” Geographical scope in five Regions: South East Europe, Southern Caucasus, Moldova and Ukraine; Central Asia; Middle East; North Africa; South East Asia.

Concluding remarks

The growing awareness of the importance of the human factor in sustaining a nuclear (or CBRN) security regime is leading to an increasing number of security centres, NSSCs and CoE. In a world in which resources are clearly scarce and mutual assurances essential, international cooperation and coordination is the only practical road toward effective and sustainable security regimes. The Gift Basket on NSSC/CoE, presented by Italy and co-sponsored by 31 countries, is an important recognition of the importance of this objective.

Franca Padoani
ENEA, Technical Unit for Reactor Safety and Fuel Cycle Methods - Reactor Core and Shielding Analysis and Design Laboratory

Antonietta Rizzo
ENEA, Technical Unit for Reactor Safety and Fuel Cycle Methods - Fuel Cycle Safety and Security Laboratory

references & notes

[1] F. Padoani, 2014, The Nuclear Security Summit process: the turn of the screw (this issue).
[2] D. Nikonov, 2013, The international Nuclear Security Education Network (INSEN) and the Nuclear Security Training and Support Centre (NSSC) Network, Technical Meeting IAEA.
[3] A. Mignone, 2013, The European Union’s Chemical, Biological, Radiological and Nuclear Centres of Excellence Initiative, EU Non-Proliferation Consortium.

Costruire dei team di *Advisors* e *First Responders* a supporto dei vertici decisionali per far fronte a situazioni di emergenza dovute ad eventi chimici, biologici, nucleari ed esplosivi

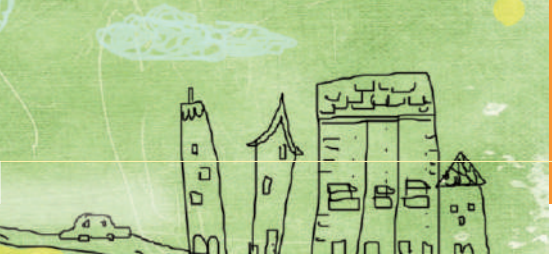
Il Dipartimento di Ingegneria Industriale e la Facoltà di Medicina e Chirurgia dell'Università di Roma Tor Vergata si sono occupati della necessità, da parte degli esperti del settore, di far fronte a eventi di natura Chimica, Biologica, Radiologica, Nucleare, esplosiva (CBRNe), creando nel 2009 il primo corso universitario finalizzato alla formazione di CBRNe Advisors a supporto dei vertici decisionali. Tale corso si è evoluto nel tempo, entrando ufficialmente in convenzione con la Presidenza del Consiglio dei Ministri, il Ministero dell'Interno, il Ministero della Difesa, l'INGV e l'ENEA, ed ottenendo il riconoscimento dello status di NATO SELECTED, oltre al primo accordo di collaborazione di questo tipo con l'Organization for the Prohibition of Chemical Weapons (OPCW). Il bisogno della comunità internazionale di rafforzare le misure di safety e security è stato il motivo principale per cui il Direttivo del Master ha deciso di suddividere il corso italiano in due Master Courses internazionali: un corso di primo livello, 1st-Level Master Course in Protection against CBRNe events, dedicato alla formazione di CBRNe First Responders altamente qualificati, e un corso di secondo livello, 2nd-Level Master Course in Protection against CBRNe events, dedicato alla preparazione di CBRNe Advisors a supporto dei vertici decisionali (le iscrizioni per l'anno 2014/2015 sono già aperte). Il presente articolo illustra le minacce attuali, nonché gli obiettivi e l'ottica di questo Progetto Internazionale.

Building a team of Chemical, Biological, Radiological, Nuclear, explosive events Tech Advisors and First Responders to support top decision makers during emergencies

The Department of Industrial Engineering and the Faculty of Medicine of the Rome University of Tor Vergata took up the expert needs to face Chemical, Biological, Radiological, Nuclear, explosive (CBRNe) events and created, in 2009, the first Academic Course aimed at training CBRNe Tech Advisors for Decision Makers. The course has grown during these years getting the Official Cooperation of the Italian Presidency of Ministry, Ministry of Interior, Ministry of Defence, INGV, ENEA and the status of NATO SELECTED and, the first agreement of this kind, with the Organization for the Prohibition of Chemical Weapons (OPCW). The International safety and security needs have been the principal reasons that convinced the Directive Board of the Master to split the Italian Course into two separate International Master Courses in "Protection against CBRNe events" – a First Level course to prepare CBRNe First Responders – and a Second Level course to prepare CBRNe Tech Advisors (the enrollment for 2014/2015 is already open). The current threats, the Mission and the Vision of this International Project are presented in this paper.

DOI: 10.12910/EAI2014-101

L. Palombi, C. Bellecci, A. Malizia, V. Cusmai, V. Rossi, T. Labriola, E. Farrugia, F. Campopiano, F. Salerno, V. Trombadore, L.Cadoni, G. Rezza, R. Fantoni, S. Sandri, M.Chiappini, A. Gucciardino, F. D'Amico, D. Rothbacher, M. Carestia, D. Di Giovanni, O. Cenciarelli, C. Russo, C. Perrimezzi, P. Gaudio



Introduction

The Department of Industrial Engineering and the School of Medicine and Surgery of the Rome University of Tor Vergata organize two international Master courses in "Protection against CBRNe events", aimed at creating a community of experts, each one with its own specific competence, and supported by a common knowledge of the subject. The courses are divided into two degrees, the first level and second level, dedicated to First Responders and Tech Advisors for Top Decision Makers, respectively. The main purpose of these courses is to integrate the skills and expertise by means of training and by conducing didactical and research activities in the areas of Safety and Security through a project. This is the mission of the International Master Courses in Protection against CBRNe events (Fig. 1):

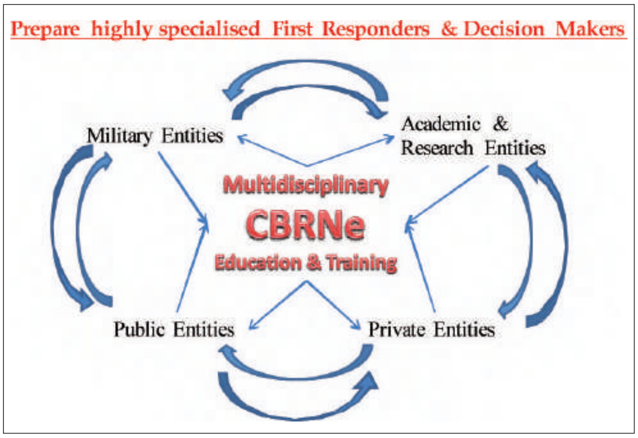


FIGURE 1 Mission of International Master Courses
Source: www.mastercbrn.com

Civilian, military and industrial experts together at university

Several extreme events require high-qualified experts to intervene quickly, directly as first responders, or indirectly as advisors to decision makers. The assessment of individual risk is a correct approach for an analytical examination of the scenario, but the possibility of mixed scenarios cannot be ruled out. CBRNe agents can cause damage by harming people, flora and fauna either by themselves or as a combination, making it extremely difficult to identify a complete list of possible scenarios. In the effort of giving an answer to all these complex aspects, during the academic year 2009-2010 at the Rome University of Tor Vergata, the Department of Industrial Engineering, together with the School of Medicine and Surgery, decided to start a Second Level Master Course in Protection against CBRNe events. This course focused on the training (both theoretical and practical) of highly specialized experts in the field of CBRNe safety and security. During the first four years, the vision of the Master course has continuously developed (Fig. 2):

The course mission and vision led to create a new prospective of collaboration, allowing experts from the Civilian, Military and Research environment, to have a direct and constructive debate in the framework of the Master Courses in Protection against CBRNe events. During these years, collaborations are growing constantly, reaching the present level of excellence by signing official collaboration agreements with:

- Presidenza del Consiglio dei Ministri (Prime Minister's Office);
- Ministero della Difesa (Ministry of Defence);
- Ministero dell'Interno (Ministry of The Interior) [On July 18th, 2013, the Rome University of Tor Vergata and the Ministry of the Interior, signed a cooperation agreement under which the Public Security Department and the Fire Fighters Department will support the University's Master Courses in protection against Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) events. This cooperation agreement has enhanced the technical skills sectors of the Public Security Department and the Fire Fighters Department. This strong institutional footprint refers to the interoperability between the Departments of the Interior Ministry, called to ensure everyone for their expertise, aspects of Security (Public Security Department) and Safety (Fire Fighters Department).

■ **Contact person: Andrea Malizia**
malizia@ing.uniroma2.it

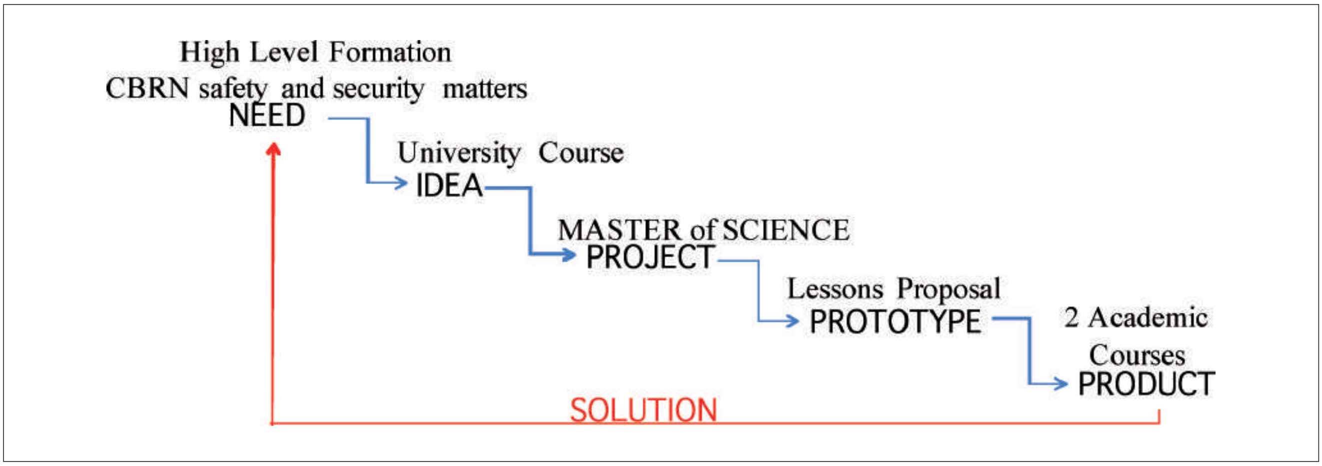


FIGURE 2 Vision of International Master Courses
Source: www.mastercbrn.com

In particular, are invoked, already doctrinally, aspects of preservation and national security, insured as institutionally expected, under the aegis of the Ministry of the Interior, with the involvement of other relevant Agencies and Institutions];

- ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development);
- Istituto Nazionale di Geofisica e Vulcanologia (National Institute for Geophysics and Vulcanology);
- Istituto Superiore di Sanità (National Health Institute);
- Comitato Parlamentare per l'Innovazione Tecnologica (Parliamentary Committee for Technological Innovation);
- University consortia: CRATI scrl; MARIS scarl; SCIRE scarl;
- and with International Entities and Facilities:
- NATO JCBRN Centre Of Excellence – (Czech Republic)
- NATO School of Oberammergau (Germany)
- HotZone Solutions (The Netherlands)
- VVU-026 Sternberk (Czech Republic)
- Seibersdorf Laboratories GmbH (Austria)
- Chernobyl Centre (Ukraine)

The high level of these International Collaborations led the Master Course to accept the challenge of growing need for training in the CBRNe safety and security context, and to split the course in two: one to prepare highly specialized First Responders (1st level course) and the other, to prepare highly specialized Decision Maker (2nd level course). *On 16 April 2013, NATO HQ SACT (Supreme Allied Commander Transformation), located in Norfolk, Virginia, USA, granted the NATO "SELECTED" accreditation to both CBRNe Master Courses [1]*. The International CBRNe Master Course (1st level Master Course) and the Executive CBRNe Master Course (2nd level Master Course) will be included in the NATO Education and Training Opportunities Catalogue (ETOC). The assessment by NATO SACT JFT (Joint Force Trainer) of both Master Courses – which include, among others, CBRN live agent training carried out in cooperation with international partners – have been conducted according to the existing NATO policy, doctrine, and directives. The course fulfilled all the requested requirements for the accreditation by NATO.

The NATO selected accreditation implies that:

- The Master Courses in Protection against CBRNe events meet NATO's training requirements;
- The Master Courses in Protection against CBRNe events can be delivered outside a NATO training establishment;
- The Rome University of Tor Vergata designed and developed the Master Courses and retains their ownership.

On June 20th, 2013, the University of Tor Vergata and the OPCW signed a cooperation agreement, under which the OPCW Technical Secretariat will support the University's Master Courses in protection against Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) events. This is the first agreement ever in the world between an University Course and OPCW [2]

From desk to field and back: exchanging experiences in the face of a real emergency

The old Italian Edition of the II Level Master Course has been closed and substituted with:

- **The First Level Master Course** that aims at providing participants with suitable technical and operational skills and knowledge, to become key players in the new area of CBRNe risks. In order to participate in the Master Course and obtain the final degree (which has legal value according to the Italian law), candidates must have a Bachelor's degree (180 point recognized according to the ECTS), or titles certifying the expertise of students coming from their work experience. The course is divided into 12 modules:
  - Module 0 - Introduction to CBRNe risks - the point of view of a first responder - Rome (Italy);
    Students are involved in training activities with Air Force, Navy (Fig. 3) and Fire Brigades (Fig. 4).
  - Module 1 - Biological events - Rome (Italy).
  - Module 2 - Radiological and Nuclear events - Rome (Italy).
  - Module 3 - NBC School of Rieti - Rieti (Italy).
  - Module 4 - Chemical events and explosive events - Rome (Italy).
    In the previous editions students also participated to decontamination tests (Fig. 5).
  - Module 5 - JCBRNE COE - Vyskov (Czech Republic).
  - Module 6 - VVU + Seibersdorf - Vyskov (Czech Republic) + Vienna (Austria).
    A delegation of students from the 3rd and 4th editions of the Master Courses attended the course "Training for First Responders Trainer" at the JCBRN CoE in Vyskov (Figs. 6 and 7).
    Students from the previous edition of the Master also took part in the First Course with Live Training Agents (LAT) at VVU Vyskov, run by Hotzone Solutions Group, and had the chance to exercise with Sarin, Yprite and VX (see Fig. 8). Furthermore Dott. Luca Rotondi, an attendee of the 4th edition of the Master Course, was the first deaf person able to complete a NATO course and a Training with LAT [3].
  - Module 7 - Private factories - Rome (Italy).
  - Module 8 - Medical first aid and emergency planning - Rome (Italy). The students, in previous editions, already participated in training for medical first Aid (see Fig. 9).
  - Module 9 - Software and DSS - Rome (Italy).
  - Module 10 - Investigation and Communication - Rome (Italy).
  - Module 11 - Chernobyl center - Chernobyl (Ukraine).

FIGURE 3 Master students on the Italian aircraft carrier "Cavour"
Source: www.mastercbrn.com

FIGURE 4 Master students inside of a Firefighter Brigades mobile laboratory
Source: www.mastercbrn.com

FIGURE 5 Decontamination training activities
Source: www.mastercbrn.com

FIGURE 6 Master students during a training at COE
Source: www.mastercbrn.com

  - Stage.
  - Final thesis dissertation.
- **The Second Level Master Course** that aims at providing participants with appropriate technical, cognitive and operational skills in order to train key figures in the field of CBRNe risk, able to coordinate at tactical and strategic levels. To participate in the Master Course and obtain the official title (which has legal value according to the Italian law), candidates must have a 300 ECTS point Master degree, or titles that recognize the expertise of students coming from their work experience.

  The course is divided into 7 modules:
  - Module 0 - CBRNe International Safety and Security Policy - Rome (Italy).

    Students are involved in high level exercise: Figure 10 shows a representative group of students at ISPRA (National Institute for Civil Protection and Environment) during an International Emergency simulation.
  - Module 1 - CBRNe Agents - Rome (Italy).
  - Module 2 - CBRNe Protection and Decontamination - Rome (Italy).
  - Module 3 - DSS for Advisors - Rome (Italy).
  - Module 4 - NATO School - Germany – Oberamergau.
  - Module 5- Different ways to manage a CBRNe event in different continents- Rome (Italy).
  - Module 6- Medical management of a CBRNe Maxi-Emergency -Rome (Italy).
  - Module 7 - Investigation and information in case of a CBRNe events - Rome (Italy).
  - Module 8 Private Companies - Rome (Italy).
  - Remedial Session - Rome (Italy).
  - Stage.

FIGURE 7 A master student from Italian Red Cross at JCBRNE COE NATO during the field training activities
Source: www.mastercbrn.com

FIGURE 8 Master student with an operator of Hotzone Solution during a training with Live Sarin at VVU
Source: www.mastercbrn.com

- FINAL ACTIVITY – Along with the final thesis delivery, students will be involved in a 2-3-day Table Top Exercise that will contribute to their final evaluation.

  Among its collaborations the Master Course won, together with Scuola Sant'Anna di Pisa and the Italian Fire Brigades, and in collaboration with Polizia di Stato (the Italian State Police), Carabinieri corps, Civil Protection and Italian Army, an International Project to improve the Italian CBRNe system for the 7th European Framework Program [4].

  In 2013, the II Level Master Course, in collaboration with Ministry of Interior, Ministry of Defence, Italian Red Cross, INAIL and ARPA, organized the first Table Top Exercise (TTX) to evaluate the preparation of students [5].

FIGURE 9 Master students during a training
Source: www.mastercbrn.com

FIGURE 10 A master student during an International Emergency Simulation
Source: www.mastercbrn.com

Conclusions

The degrees, such as Military, Police, Fire-fighter Academy degrees etc., will be assessed on a case-by-case basis by the University's competent bodies and the Master Course's Steering Committee.

Since 2009, more than 80 students have completed the Master Degree; students come from Academic, Military and Civilian contexts, both experts and people who joined the course to acquire expertise for a new job.

During these years the collaborations between students and the teachers, the contacts with the Public, Private and Military Entities involved in the CBRNe safety and security, together with the training and strategic activities, led to the following results:

- International Collaborations among experts for improving the emergency system;
- International Patents due to ideas born during the Master Course;
- Realization of International CBRNe network;
- Realization of new products from companies to end-users;
- Research activities and Scientific Publications in International peer-to-peer Journals;
- Raising of International Funds;
- New job opportunities (95% of the students attending the Master Course get a job today).

The ultimate goal is to experience the collaboration with Companies, Laboratories and International Organizations and let the courses deliver a preparation that goes into the world of Safety and Security and CBRNe relying on the University of Tor Vergata as a neutral focal point for the coordination of these activities. This is the final purpose of the International Master Courses in Protection Against CBRNe events.

Acknowledgements

Special Acknowledgments to all the Entities and the people that put so much effort to realize this ambitious project, in particular to the Didactical Board and to all the students of the present and former editions. Further information available at: www.mastercbrn.com. Enrollment for A.Y. 2014/2015 OPEN.

Andrea Malizia, Fabrizio D'Amico, Dieter Rothbacher, Mariachiara Carestia, Daniele Di Giovanni, Orlando Cenciarelli, Carlo Bellecci, Pasqualino Gaudio
University of Rome Tor Vergata, Industrial Engineering Department

Vittorio Cusmai
Italian Defence Staff, Division I

Vincenzo Rossi
Italian Ministry of the Interior

Tiziano Labriola
Italian Presidency of the Council of Ministers

Emanuele Farrugia
Italian Ministry for Foreign Affairs

Francesco Campopiano
Italian Presidency of the Council of Ministers, Civil Protection Dept.

Franco Salerno
Joint NBC Defence School

Vincenzo Trombadore
Italian Ministry of the Interior, Public Security Dept.

Luciano Cadoni
Italian Ministry of the Interior, Firefighters Dept.

Giovanni Rezza
ISS - Istituto Superiore di Sanità (Italian National Institute of Health)

Roberta Fantoni
ENEA, Technical Unit for the Development of Applications of Radiation

Sandro Sandri
ENEA, Radiation Protection Institute - Radiation Protection for Nuclear Fusion Plants and Large Accelerators Laboratory

Massimo Chiappini
Istituto Nazionale di Geofisica e Vulcanologia (INGV)

Antonio Gucciardino
University of Tor Vergata, Scientific Board of International Master Courses in Protection Against CBRNe events, Department of Industrial Engineering and School of Medicine and Surgery

Colomba Russo, Carlo Perrimezzi
Crati Scrl - Consorzio per la ricerca e le applicazioni di tecnologie innovative

Leonardo Palombi
University of Rome Tor Vergata, School of Medicine and Surgery - Department of Biomedicine and Prevention

references & notes

[1] http://www.mastercbrn.com/news/69/natoselected-accreditation-granted-to-both-master-courses/
[2] http://www.mastercbrn.com/news/75/university-of-rome-tor-vergata-and-opcw-concluded-a-cooperation-agreement/
[3] http://www.mastercbrn.com/news/88/live-agent-training-pilot-module/
[4] http://www.mastercbrn.com/page/73/strengthening-cbrn-response-in-europe-by-enhancing-on-site-cooperation-between-safety-and-security-organizations-an-italian-pilot/
[5] http://www.mastercbrn.com/news/181/table-top-exercise/