

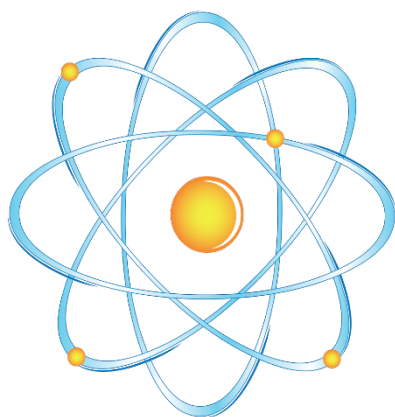
JRC TECHNICAL REPORTS

National and cross-border expert support for nuclear security

*European Reference
Network for Critical
Infrastructure Protection
Radiological and Nuclear
Threats to Critical
Infrastructure Thematic
Group*

Tengblad, O., CSIC, Spain
Peräjärvi, K., STUK, Finland
Toivonen, H., HT Nuclear, Finland
Tagziria, H., JRC, Italy
Schoech, H., CEA, France
Eisheh, J. -T., BfS, Germany
Kröger, E. A., BfS, Germany

2019



The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

This publication is a technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information

Name: Georgios Giannopoulos
Address: via E. Fermi 2749, 21027, Ispra (VA), Italy
Email: georgios.giannopoulos@ec.europa.eu
Tel. +39 0332786211

JRC Science Hub

<https://ec.europa.eu/jrc>

JRC115110

EUR 29602 EN

PDF ISBN 978-92-79-98659-8 ISSN 1831-9424 doi:10.2760/365006

Luxembourg: Publications Office of the European Union, 2019

© European Union, 2019

Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU (OJ L 330, 14.12.2011, p. 39).

For any use or reproduction of photos or other material that is not under EU copyright, permission must be sought directly from the copyright holders.

How to cite this report: Author(s), *Title*, EUR (where available), publisher, publisher city, year of publication, ISBN (where available), doi (where available), PUBSY No.

Contents

Abstract	5
1. General introduction	6
1.1. References	9
2. Iodine-125-contaminated card pieces.....	10
2.1. The organisation of radiation protection in Germany	10
2.2. Radiation portal monitor alert	10
2.2.1. The second find in 2016	11
2.3. The investigation.....	12
2.3.1. Characterisation of the circular card pieces	13
2.3.2. The purpose of the circular card pieces.....	14
2.4. References	15
3. Cross-border interception of illicit trafficking	16
3.1. Introduction	16
3.2. Scenario	16
3.3. Timeline	19
3.3.1. Access of first responders to the site	21
3.3.2. Radioactive sources	21
3.4. Illustrations	22
3.5. Key points	23
3.5.1. Bilateral agreement and training	23
3.5.2. The French reachback centre	23
3.6. Data transmission and storage.....	24
3.7. Complementary actions	24
3.8. Conclusions	25
4. Reachback demonstration: Magic Maggiore.....	26
4.1. Introduction	26
4.2. Objectives of the demonstration	26
4.3. The demonstration scenario and actors.....	27
4.4. The scenario in four parts	28
4.4.1. Part I.....	28
4.4.2. Part II.....	30
4.4.3. Part III.....	30
4.4.4. Part IV.....	31
4.5. Conclusions	32
5. REPO technology and the Estonia-Finland cross-border reachback demonstration ..	33
5.1. Introduction	33
5.1.1. REPO project 2012-16	34
5.2. Estonia-Finland cross-border reachback demonstration	35
5.3. Conclusions	37
6. Exercises and testing nuclear detection capabilities using an electronic platform	38
6.1. Introduction	38
6.2. Simulation of threat scenarios	39
6.3. Search for radioactive material in a virtual world	39
6.4. Discussion	41
6.5. References	42
7. National and international cooperation — role of expert support	43
7.1. Information sharing	43
7.2. Political-level agreements and cooperation between states.....	44

7.3. CONOPs and expert support in nuclear security	44
7.4. Technical tasks for expert support	45
7.5. Benefits of reachback.....	46
7.6. Requirements and capabilities of expert support	46
7.7. Different types of reachback centres	46
7.8. References	47
List of abbreviations	49
Appendix 1. List of items needed for the development of reachback capabilities.....	50
Appendix 2. List of publications of the ERNCIP RN Thematic Group, 2014-18	52

Abstract

The role of technical, scientific and operational expert support is analysed through case studies and scenarios. The technology demonstrations show that cooperation between competent authorities is necessary for the successful handling of a nuclear security event both nationally and internationally. An event that occurs in one state could also affect other states. For this reason, high-level agreement between states is necessary to allow the horizontal exchange of information during a nuclear security event. Expert support is a crucial cross-cutting element of a nuclear security detection architecture. This report attempts to identify the basic elements and capabilities of a national expert support system.

1. General introduction

The EU has recently faced a range of terrorist threats and attacks of a violent nature. Radicalised groups have carried out attacks in the EU with the aim of maximising both the number of victims and the psychological and economic impacts on society. Thus far, chemical, biological, radiological and nuclear (CBRN) materials have not been used, but their potential is daunting, as demonstrated by the Novichok chemical attack in Salisbury, the United Kingdom, in March 2018. Radiological and nuclear (RN) agents, such as polonium, as used in the 2006 Litvinenko case, are not only a health hazard to the individuals directly affected but may also have wider societal consequences, causing wide-scale damage to the economy and the environment.

Information sharing between competent authorities is of vital importance for nuclear security. Joint protocols on data structures and data handling can ease the flow of information. Efficient and secure information sharing is necessary to prevent an attack or other type of crime and enable the efficient use of available expertise and equipment. For a timely response, the authorities need to cooperate by having joint protocols and data structures in place. However, the implementation of such protocols and structures has turned out to be difficult, particularly at the international level.

There is a strong need to maintain the skills of experts, first responders and front-line officers (FLOs) through continual education, exercises and training, and also by validating joint procedures agreed between the different units involved, by testing detectors and by advising first responders on which detector is best suited to a particular mission.

Not all countries have the capabilities required to develop and implement advanced detection systems within their borders and thus identify material out of regulatory control (MORC) and prepare themselves for various types of criminal activity. For efficient expert support (reachback), there is a strong need to standardise data collection and storage and for the rapid distribution of the data analysed across EU borders. If standard protocols and efficient data transmission solutions were in place, efficient cross-border expert nuclear security support could be arranged. Because of the variety of responsibilities across national borders, expert support capabilities need to be defined early, well before an actual event.

The work presented in this report follows the guidelines for the implementation of the new European Commission action plan on chemical, biological, radiological, nuclear and explosive (CBRNE) security risks [1.1]. In particular, the following commitments outlined in this plan support the development of nuclear security detection architectures (NSDAs):

- 'Strengthen risk-based customs controls to intercept dangerous CBRN materials at the border' (1.2);
- 'Reinforce nuclear security capacities and networks' (2.9);
- 'Develop cooperation with specialised international organisations' (3.3).

Furthermore, the EU security industrial policy action plan (4.1.1., Action 1) [1.2] concludes that the European security industry suffers from market fragmentation. To move closer to a single market, Europe-wide standardisation of and certification schemes for security products are necessary.

Because of the variety of roles and responsibilities of nuclear experts, three complementary categories of expert support have been defined [1.3]:

1. technical support, which includes detection systems, the deployment and maintenance of equipment and the training of operational forces;

2. scientific support, which assesses, offers in-depth analysis of and adjudicates on alarms at the request of FLOs;
3. operational support, which is integrated into operative units, such as CBRNE teams, law enforcement investigators and crime-scene management teams.

Decision-makers, incident commanders, FLOs and experts can share technical data in a variety of ways, including through formally established communication tools (methods such as the use of encryption, secure cloud services or dedicated mobile networks) or informal methods. Regardless, protocols for both on-scene operators and remote technical experts should clearly define the procedures for sharing technical data. In addition, information exchange is involved in many other aspects of expert support, such as deploying instruments and improving cooperation over borders, as well as the national, regional, bilateral or international exchange of information on prevailing threats. FLOs must know when and how to request technical or scientific expert support and there must be established procedures to facilitate the quick transmission of information alerts and instrument alarms.

At the Magic Maggiore Technical Reachback Workshop held in Ispra, Italy, in 2017 [1.4], the following 'best practices' for implementation in EU Member States were formulated for consideration:

- include expert support in national-level information-sharing protocols, as well as in emergency response coordination mechanisms;
- conduct joint exercises (including tabletop exercises and drills) that test and evaluate interactions between technical experts, law enforcement agencies and decision-makers;
- conduct peer-to-peer exchange, training sessions and exercises with regional partners and international organisations to enhance information-sharing procedures and advance relationships between partner nations;
- identify and make use of advanced regional or international partners for reachback support instead of developing complex and wide-ranging national capabilities.

New technologies have made it possible to develop more efficient detection systems. In particular, digitalisation and the internet of things (IoT) provide great opportunities for cooperation at a technical level. The IoT communication layer for detectors and detector networks enables the continuous low-level online automation of early warnings and efficient high-level expert support on technical and scientific matters. Big data and related data mining in conjunction with automated online monitoring have the potential to enable observations to be analysed over longer periods, making early warnings and the early prevention of prevailing illegal activities possible. For nuclear security, data security is of the utmost importance, and there must be mechanisms to ensure that information is shared securely nationally and internationally.

There is a need for a concept of operations (CONOP) based on joint protocols for data structures and data handling, including procedures on how different units are to interact with each other to ensure an efficient flow of information across borders in close cooperation with decision-makers, FLOs and nuclear experts. The potential technical and scientific themes to be considered are as follows:

- novel detection solutions;
- digitalisation of the information already at the detector using standardised formats;
- the use of the IoT or another solution for the automatic transfer of data from detector to data server, taking into account related cybersecurity issues;

- automated analysis of the digitised information and distribution of information to different technical/scientific centres for expert support services;
- big data and data mining.

The Thematic Group for Radiological and Nuclear Threats to Critical Infrastructure (the ERNCIP RN Thematic Group), part of the European Reference Network for Critical Infrastructure Protection (ERNCIP) project [1.5], has over the last 5 years focused its efforts on the areas outlined below.

- List-mode data acquisition based on digital electronics: a time-stamped list-mode data format provides significantly more added value than a more conventional spectrum format. It improves source localisation, allows signal-to-noise optimisation and allows noise filtering, and some new gamma and neutron detectors require list-mode data to function. The list-mode approach also allows the precise time synchronisation of multiple detectors enabling, for example, simultaneous singles and coincidence spectrometry, such as singles gamma and UV-gated gamma spectrometry.
- Remote-controlled radiation measurements and sampling using unmanned vehicles: several measurement and sampling scenarios are too risky for humans and therefore such technology could be used instead. Applications envisaged include measuring or sampling at reactor or other accident sites, and dirty bombs before and after explosion, and searching for sources out of regulatory control.
- Expert support for field teams, i.e. data moves instead of people and samples: this would allow fast and high-quality responses to be achieved with fewer people. However, agreed formats and protocols have to be available for efficient reachback.
- Novel technologies: recent technological developments have occurred at a fast pace in the area of radiological detection. New types of sensors have been developed for the detection of neutron and gamma radiation, and their capabilities are further improved by integration, either at the sensor level (arrays) or at the network level (reachback).

The achievements have been published and are listed at the end of this document.

The current paper aims to describe the role of expert support in nuclear security. Sometimes local experts cannot handle a specific threat situation or lack the necessary equipment and software. In such cases, technical, scientific or operational expert support could be obtained from other Member States to make the response more efficient. Various examples are introduced, namely analyses of case studies or scenarios implemented through exercises or virtual reality (simulations). The aim is to raise awareness of the need for cross-border expert support in nuclear security.

1.1. References

- [1.1] Ec.europa.eu, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf
- [1.2] Communication from the commission to the european parliament, the council and the european economic and social committee security industrial policy action plan for an innovative and competitive security industry ipex.eu com/2012/0417, <http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20120417.do>
- [1.3] Tengblad, O., Peräjärvi, K., Toivonen, H. and Gattinesi, P., *After-action analysis of the Magic Maggiore Workshop on expert support and reachback*, Publications Office of the European Union, Luxembourg, 2017.
- [1.4] JRC, 'Magic Maggiore — Technical Reachback Workshop', Ispra, Italy, 16 March 2017, Joint Research Centre, European Reference Network for Critical Infrastructure Protection, <https://erncip-project.jrc.ec.europa.eu/events/magic-maggiore-technical-reachback-workshop>
- [1.5] ERNCIP Project, <https://erncip-project.jrc.ec.europa.eu>

2. Iodine-125-contaminated card pieces

J.-T. Eisheh, E. Kröger, A. Rupp, and J. Gregor
Bundesamt für Strahlenschutz, Germany

Abstract

This chapter describes a Concept of Operations (CONOPS) utilizing, as an example, a real case that occurred in Berlin in the early 2014. It sketches the implementation of a German states detection strategy. The CONOPS outlines how the different parts of the detection architecture and the personnel are deployed to reach the states detection goals.

2.1. The organisation of radiation protection in Germany

The German Federal Office for Radiation Protection (Bundesamt für Strahlenschutz, BfS) supports the radiation protection authorities and other authorities of the German states ('Länder') in the event of radioactive MORC, misuse of radioactive material or (suspected) threats involving radioactive material [2.1]. Assistance to a state ('Land') is granted after a formal request. In the majority of cases, the responsibility for the investigation remains with the local authorities. BfS supports the competent authorities by providing expert advice and laboratories for handling contaminated evidence and spectrometric and/or radiochemical analysis.

An annual expert information exchange organised by BfS is conducted together with police, radiation experts of the Länder and experts of other authorities who might be involved in incidents involving MORC (e.g. customs authorities, fire brigades) to facilitate knowledge transfer regarding capabilities and procedures and to promote interauthority cooperation.

2.2. Radiation portal monitor alert

In 2014, the operator of an incineration plant in the German Land of Brandenburg received an alarm from their radiation portal monitor (RPM). In accordance with standard procedure, the competent authority for Brandenburg was contacted and a search for the source of the alarm was started.

Circular pieces of playing cards were subsequently identified as the cause of the alarm and the contamination was initially thought to be Nickel-63 (Ni-63) or Iron-55 (Fe-55). However, it remained unclear what use the card pieces had and why they were contaminated. The find was discussed by the Brandenburg authorities



Figure 2.1. Contaminated card pieces (second find in 2016).

(radiation protection and police authorities) during a regular information exchange with experts from BfS. It was agreed that the samples would be sent to BfS for further examination and radiochemical analysis. The BfS lab identified the contamination as iodine-125 (I-125) (see box 2.1) with gamma spectrometry and radiochemical analysis. Neither Ni-63 nor Fe-55 was found to be above the detection limit. The analysis also established that the amount of I-125 found was above the legal limit for handling without a license in Germany. No impurities were detected. An investigation into a possible environmental crime was started by the Criminal Police Office of Brandenburg (LKA-Brandenburg).

Box 2.1. Information about the isotope Iodine-125 [2.2].

Iodine-125	
I-125 decays by electron capture (daughter Tellurium-125, stable) and emission of low-energy gamma and X-ray radiation.	
I-125 is used as a marker in medical or biological studies and for brachytherapy, for instance for the treatment of prostate cancer through the implantation of 'seeds'.	
I-125 is manufactured by the irradiation of Xe-124 in a nuclear reactor and subsequent radiochemical separation.	
The German legal activity limit, above which a license is required, is 1 MBq.	
γ emission	35.4922 keV
X-ray emission	27.4726 keV, 27.202 keV, 31.0589 keV, 31.7623 keV
Half-life	59.388 days

2.2.1. The second find in 2016

In 2016, another portal monitor alarm caused by I-125 occurred at the same incinerator plant in Brandenburg. Since contact with the Brandenburg authorities had already been established, BfS was immediately informed and supported the search for the source of the alarm by providing personnel and equipment onsite. Several contaminated circular card pieces, together with some other material (food, paper) that was also contaminated and related to the card pieces, were found, see Figures. 2.2a-2.2b.



Figure 2.2a. Searching domestic for contamination can be very time consuming.

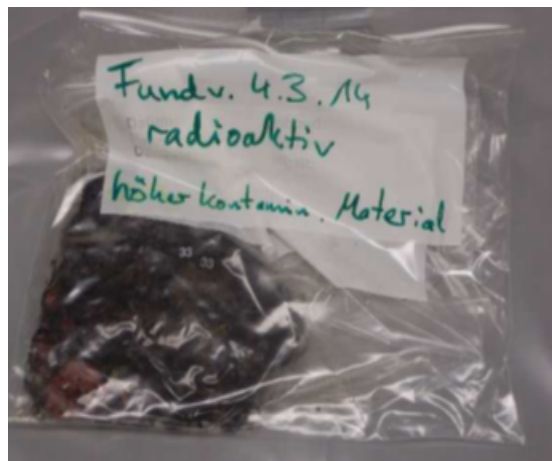


Figure 2.2b. Packaging and labeling evidence.

All items were packaged and transported to the BfS laboratory in Berlin. With the help of the Brandenburg police, the items were unpacked, labelled and examined in a controlled area for the handling of open radioactive material. The documentation and examination of the items were led by the police, while BfS ensured that the personnel followed proper radiation protection procedures and recorded the dose rate from the items. Gamma spectrometry with planar n-type detectors was used to identify the radionuclide and determine the amount of activity associated with each circular card piece.

2.3. The investigation

The lorry that caused the second alarm was transporting waste from businesses in Berlin (another German Land, separate from Brandenburg). Therefore, authorities in Berlin were contacted and, after an information exchange, the investigation (including all the information collected) was handed over to the Criminal Police Office of Berlin (LKA-Berlin). By analysing the truck's route, the possible area from which the contaminated card pieces had originated could be substantially narrowed down. At the end of 2017, Berlin police searched a property (restaurant) and found I-125-contaminated card pieces (Figure 2.3), hole punchers and some residual (I-125) contamination. The search team was accompanied by radiation protection personnel from Berlin, who ensured the radiation safety of police officers during the operation and assisted with crime scene work where necessary. Three persons had to be checked for possible I-125 incorporation by BfS. In addition, the Berlin radiation protection authority closed part of the property that had been searched to the public because of contamination. The operation was jointly planned and executed by the police and radiation protection officers. A standard approach to this kind of joint operation can be found in [2.3] and [2.4].



Figure 2.3. 'Radioactive Playing Cards': Berlin Police informed the public with all relevant details in their newsfeed on social media [2.5].

2.3.1. Characterisation of the circular card pieces

Beyond the immediate needs of the investigation, BfS was asked to further characterise the circular card pieces, . The aim of this effort to characterise the cards was to determine — if possible — the age and the origin of the radioactive material and to gain more knowledge about how the cards were manufactured.

Figure 2.4. The distribution of the contamination was determined by moving small pieces of solder as shielding over a card piece or via the use of improvised collimators (not shown).



The card pieces could be divided into two groups: one that had card pieces with relatively high levels of activity and that had been confined to a small area on one side (namely 'primary contamination') and one containing card pieces that demonstrated only slight contamination and a uniform distribution of the contamination over the complete surface (most likely from cross-contamination). The distribution of the contamination was determined by moving small pieces of solder over a card piece or via the use of improvised collimators (see Figure 2.4).

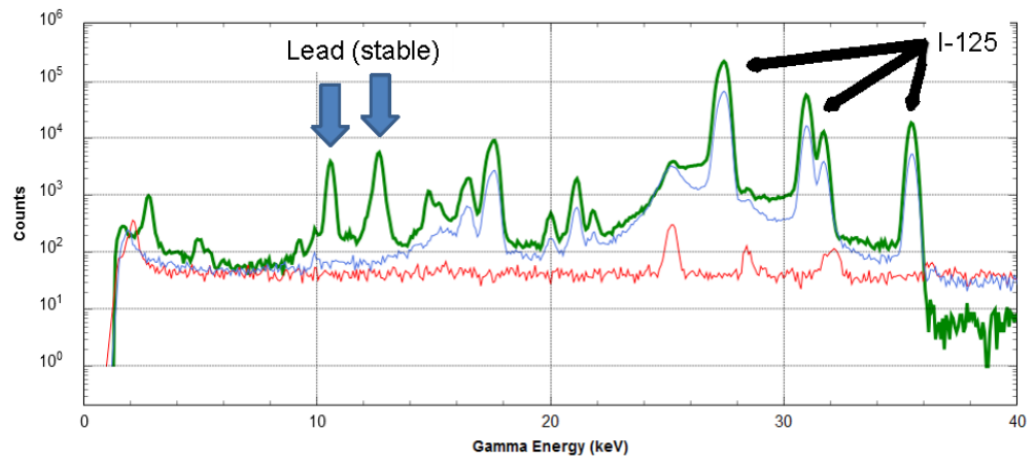


Figure 2.5. The gamma spectrum of a card piece with primary contamination.

The gamma spectra of the card pieces with primary contamination were recorded with low-energy high-purity germanium (HPGe) detectors (Figure 2.5). The spectra show X-ray peaks of stable lead. These card pieces were also slightly heavier than those without primary contamination. To explain these findings further, X-ray radiography was used. This revealed that the card pieces with primary contamination contained a small disk of lead foil (approximately 20 μm thick), see Figure 2.6. This shielded the radiation and made it easier to determine which side of the card piece was facing upwards.

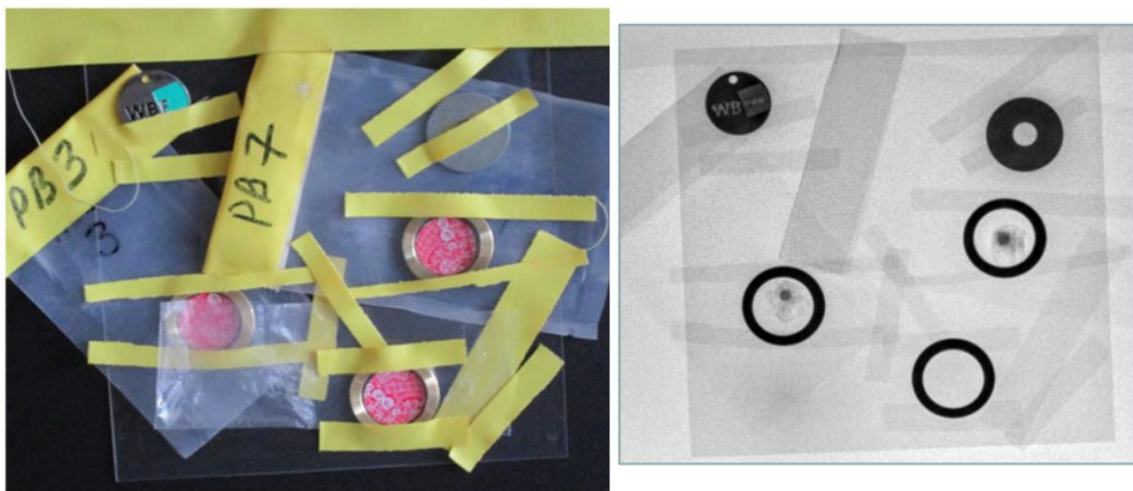


Figure 2.6. Setup (left) and result (right) of the X-ray radiography: card pieces with primary contamination show a round object. The tape was used to fix the card pieces and the metal rings make the pieces easier to find in the picture.

2.3.2. The purpose of the circular card pieces

The circular card pieces seem to have been used as 'binary dice' for the game of *chơi xúc đĩa* (Figure 2.7), which is popular in the Vietnamese expatriate community in Germany. The player of a game of this sort with manipulated card pieces can distinguish which side

of the circular card piece is facing upwards by using a radiation detector hidden in his or her sleeve and gain an advantage.



Figure 2.7. The game of *chơi xóc đĩa*. The bowl is moved over the plate and held in place while the circular pieces are shaken. The players bet on how many card pieces will lie facing upwards or facing downwards after being shaken. The contaminated card pieces allow secret detection through the bowl. After all bets are placed, the bowl is moved aside to reveal the circular card pieces (shown).

An online search shows that this type of manipulation in gambling is not restricted to Germany. Other international finds of playing cards contaminated with I-125 show that the phenomenon remains an important and pressing topic for customs, police and radiation protection authorities. In addition, it is important for hospitals to be aware that the misuse of I-125 is an issue. Unfortunately, security in terms of preventing I-125 misuse is not guaranteed worldwide at the present time.

2.4. References

- [2.1] Information about BfS and its support for the response to nuclear security events can be found at: BfS - Homepage http://www.bfs.de/EN/home/home_node.html
- [2.2] Information taken from: NUCLÉIDE-LARA on the web (2018) <http://www.nucleide.org/Laraweb/index.php>
- [2.3] IAEA, 'Radiological crime scene management implementing guide', IAEA Nuclear Security Series No 22-G, 2014, Radiological Crime Scene Management | IAEA, <https://www.iaea.org/publications/10717/radiological-crime-scene-management>
- [2.4] IAEA, 'Nuclear security recommendations on nuclear and other radioactive material out of regulatory control', Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control | IAEA <https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control>
- [2.5] Berlin Police report, facebook: <https://de-de.facebook.com/PolizeiBerlin/posts/bei-einer-routinekontrolle-einer-abfallanlage-in-rüdersdorf-wurden-im-letzten-ja/7859023282>

3. Cross-border interception of illicit trafficking

H. Schoech, CEA, France

Abstract

This chapter we deals with a hypothetical cross-border incidence between France and a neighboring country. An exercise was implemented where a lorry passing a checkpoint portal monitor triggers an alarm while crossing the border. A concept of operation is described for handling this situation.

3.1. Introduction

The case study described in this chapter is related to an exercise dealing with an interception of MORC, implemented at a crucial crossing point in France (Country A) at the border with a foreign country (Country B). This checkpoint is monitored using different technologies, including RN detection with an RPM that is under the control of Country B. If an alert is triggered by the RPM, this is followed by first-level localisation and identification with a handheld radioisotope identification device (RID) by officers from Country B. If officers from Country B ban the intercepted vehicle from entering their country, the vehicle and people implicated in transporting the material are forced back to France and entrusted to the French authorities. After the completion of information exchange between Country B and France, French procedures can be applied.

This case demonstrates how the various parties involved manage the event, using their skills, procedures and means, including through complementary measurement techniques, complementary analyses of data and adding further information to the data transmission upstream. The upstream work is also discussed, since the successful completion of this exercise (and also real case management) needs several levels of agreement between both countries. A smooth working procedure requires training and the elaboration of joint procedures across countries and across units nationwide. The French reachback centre, called 'CNER' (National Centre for Radiological Expertise), is the centre for receiving, analysing and sending data, results and advice to and from the field, in a constrained time.

3.2. Scenario

This case study aims to highlight the management of an NSDA by detailing the illicit trafficking or trafficking of an MORC across an operational border from the moment of detection until the final identification and arrest of suspects. The scenario in short is as follows:

Theme: Exercise on the interception of an MORC at a border post.
Locations: A border crossing between France and Country B and reachback centre in Paris.
Objectives: Test procedures and validate operational configuration.

Means:

- portal monitors (RPMs)
- dosimetry (personal radiation detectors (PRDs))
- handheld RIDs.

Personnel Country B:

- FLOs at the RPM
- border forces and RID expert.

Personnel Country A (France):

- FLOs
- first responders specialised in dealing with technology-related risks
- border forces and authorities
- reachback team (CNER, with 'triage' mission).



Figure 3.1. The van involved in crossing the RPM at the border (8.56 a.m.).

The main scenario is outlined below.

1. A delivery van triggers the RN alarm by passing through an RPM, at a border crossing between Country A (France) and Country B (another country), driving from Country A to Country B.
2. Country B border forces escort the van to the dedicated area, to check both the van and its occupants with an RID and contamination probes.
3. The result of the investigation (both classic and radiological) leads to the van and its occupants being refused entry to Country B. This leads to the van and its occupants being officially rejected entry to Country B and sent back to Country A (France); the van remains at the dedicated checking area.
4. Country B officially alerts France, which triggers the execution of the specific departmental area alert plan (the ORSEC border crossing plan) which involves several parties: the French border forces, the department authorities, the RN first responders, the reachback centre, etc.
5. Border forces of both countries meet and exchange information, including results from RN controls (contamination analysis, dose rate, radionuclide identification, etc.), which will be communicated to different units, especially to first responders and the French reachback centre.

6. The French reachback centre is alerted while specialised RN first responders (departmental fire officers in this case) are transferred from their station to the border crossing'
7. First responders perform RN checks in accordance with relevant procedures: contamination check, radiological buffer zone set up around the van, search for the exact location of the RN hotspot(s) on the van, acquire gamma spectrum, take photographs and investigate the documentation for the goods being transported.
8. New RN data are sent to the French reachback centre (with its 'triage' mission), to get advice on and validation of radionuclide identification.
9. The reachback centre results are returned to the RN advisor, who is in communication with the local police forces, to assess the extent of the issue and more particularly whether there is a threat or not.
10. The final situation that results is managed as follows:
 - a. there is an absence of immediate threat in this case, and only a radiological hazard that will be managed by the dedicated French unit;
 - b. the van occupants are maintained in custody;
 - c. first responders return to their station;
 - d. further investigation will be conducted by police and border forces of both countries, to find out what the intentions of the offenders' actions were, and determine eventual legal actions to be taken, etc.

The following points should be noted.

- The abovementioned 'French reachback centre' is officially named the 'Centre National d'Expertise Radiologique' (CNER) or the 'National Centre for Radiological Expertise'.
- The main mission of the CNER is to remotely support the field forces involved in RN cases and fulfil a 'triage' role in sorting out 'false', 'innocent' or 'true' alarms as a first approach, and furthermore decide whether an alarm is associated with a 'threat' or 'no threat'.
- The RN emergency centre is always ready to answer any RN emergency call, and will transfer the alert to the 24/7-on-duty reachback team who will trigger the response of the reachback centre if necessary.
- Gamma spectra are acquired by default over 300 seconds and first responders are trained to adapt this measurement-time depending on the case they are facing.
- This exercise was implemented using a real gamma source (Co-60). Training and other exercises were previously conducted with both gamma and neutron sources. The use of real sources is always preferred, to enable the real triggering of RPM alarms, and also to allow first responders to see and understand how detection devices respond to levels of ionising radiation higher than the natural background.
- When two countries are involved in an RN border-crossing event, several meetings and exchanges are needed, to ensure they are ready for a real event. Such aspects are best defined by a bilateral agreement before such an event takes place.

3.3. Timeline




The timeline illustrated in Table 3.1 starts with the RPM detection of a radiological signal from a van crossing the border. In this section, the main actions related to RN aspects are reported, from the points of view of both the field and the reachback centre.



This exercise shows that many actions are required before spectrometric acquisition can be performed, delaying the start of the reachback centre's analysis and identification work. The outcome of the analysis and identification work in this case was, however, reported back to the field in less than 20 minutes (since this case was relatively simple).


The time between the arrival of first responders on the scene and the sending of data to the reachback centre can differ from one case to another. In this case, the timeline was mainly driven by considerations such as securing and validating the area (determining whether or not, for example, personal protective equipment (PPE) or clothing was needed) before approaching.

Before the identification analysis, the reachback centre is involved in giving advice to the different players: the RN advisor in communication with the police forces, first responders in the field, fire officers at the command post, etc.

Table 3.1. Timeline of the main actions during the exercise

In the field	Local time (Western European Time)	Reachback centre	
RPM alarm triggered by a delivery van stopped at the border barriers	8.56 a.m.		
Vehicle escorted by Country B border forces to a dedicated 'doubt remove area'	9.02 a.m.		
Country B border forces start RN check: dose rate, RID monitoring	9.04 a.m.		
By default, a restricted area with a 20 m radius is marked and evacuated	9.08 a.m.		
Van occupants taken into an interrogation office (Country B)	9.13 a.m.		
French officials informed by Country B and the French 'ORSEC plan' triggered	9.37 a.m.		
French border forces arrive in the field for direct exchanges	9.47 a.m.		
	9.56 a.m.	French reachback centre (CNER) alerted through the dedicated alert line	

In the field	Local time (Western European Time)	Reachback centre	
	9.57 a.m.	On-duty experts contacted	
	10 a.m.	CNER ('triage' mission) alerted and prepare to analyse the incoming data	
Van occupants moved to the French interrogation office			
	10.07 a.m.	Point-of-contact data recovery: first responders, RN advisor, etc.	
	10.12 a.m.	First contact with first responders (on the way to border crossing)	
	10.14 a.m.	First contact with RN advisor	
First responders onsite	10.21 a.m.		
	10.25 a.m.	Contact with first responders command post and then with RN advisor	
First responders deployed onsite	10.34 a.m.		
Van occupant contamination check	10.45 a.m.		
Restricted perimeter check	10.47 a.m.		
Outside building dose-rate check	10.55 a.m.		
First responders ask for support from reachback centre: advice given and actions and radioprotection considerations confirmed		Exchange between first responders and reachback centre	
Hotspot location search	11.20 a.m.		
RID spectra acquisition, pictures taken, etc., at the identified hotspot	11.27 a.m.	Information exchange with first responder command post	
	11.33 a.m.	Spectra data, pictures, template sheets, etc., received	

In the field	Local time (Western European Time)	Reachback centre	
	11.34 a.m.	Situation point connected with RN advisor	
	11.50 a.m.	First results sent back to RN advisor	
Head RN advisor makes contact with first responder command post Agreement on the level of threat: none; only a sanitary issue about the sources, and a prosecution issue for the passengers	11.51 a.m.		
End of exercise	11.58 a.m.	End of exercise	
Debriefing of the teams		Debriefing	
All teams leave; In a real case, a reduced team may stay in place, until the source collection team arrives			

In relation to the exercise, the points described in the following sections should be noted.

3.3.1. Access of first responders to the site

Since the dedicated RN control area is located in a specifically regulated zone, the access of first responders, coming from outside, must be planned and ensured. A 'follow me' car escorts the rescue services, as a lot of conventional traffic (cars, coaches, trucks, etc.) will continue to use the various lanes at the site.

3.3.2. Radioactive sources

The gamma source was a Co-60 source with an activity of several MBq, positioned in the van, in a specific transport box, without any additional screen. For other similar exercises, other gamma sources have sometimes been used, such as Cs-137 or Ba-133. Neutron sources have also been used, to add further complexity and give first responders experience of dealing with signals that are less well known, as the devices respond differently to neutrons and to gamma radiation.

Because of the enforcement of regulations, it is quite complicated implementing an exercise involving real sources, especially the necessary 'high activity sources' that could be encountered in a real case.

This is also why the exercise is biased, as the van involved has to display a hazard sign, namely a radioactive sign, on both sides to cross the border, in accordance with official rules. Thus, for the exercise, how such a bias can be minimised must be considered, for instance by inserting 'animation sheets' at the right time. In this example, a sheet with the instruction 'Consider there are no sign on the van' was placed on the van.

3.4. Illustrations



Figure 3.2. Van being escorted to the dedicated radiation checking area (9.02 a.m.).



Figure 3.3. Country B first responder inspecting the van with an RID detector (9.04 a.m.).



Figure 3.4. Contamination check of the van occupants, by first responders.



Figure 3.5. Hotspot search and gamma spectrometry on the van, by French first responders, after having checked for contamination. At the end of spectra acquisition, data are sent directly from the RID detector to the French CNER, the reachback centre, thanks to the press of a single button.

3.5. Key points

3.5.1. Bilateral agreement and training

A cross-border alert will be dealt with more easily if agreements are made before such an event takes place. The agreement should be contained in a specific document and signed, after several exchanges between both countries, involving various authority and agency levels, at a political level of course but also at a technical level, to jointly validate, before an event takes place, the tasks that each party is responsible for and to agree on data transmission and which documents to exchange.

Joint training is also an important part of such a bilateral agreement. Before calling a system 'operational', training is needed to ensure that the procedures will fit with reality, the information can be circulated without any problems, everybody understands the procedures, on both sides of the border, and data formats are readable, etc.

3.5.2. The French reachback centre

The French reachback centre, namely CNER, has a key role, as first responders and FLOs need reactive advice while waiting for validation of identified radionuclides, before performing subsequent steps in the procedure.

The reachback centre has to be reactive, reliable and synthetic in its response. The time taken is expected to be less than 1 hour in a regular case, that is, between the reachback centre receiving the data and returning the results of the analysis. The reachback centre

gives advice not only about radiation protection, but also about transportation regulations, and therefore a transport expert is part of the department.



Figure 3.6. RN experts on duty 24/7 are analysing data coming in from the field.

3.6. Data transmission and storage

The links between the field and other places, such as the command post and the reachback centre, must be reliable, which, mostly, is not a problem nowadays. The same goes for the storage of data, especially data of different origins (point of detection or a mature detection architecture). But even if existing communication networks and storage facilities are very good, it is of the highest importance that they are regularly tested.

3.7. Complementary actions

After the first generic steps of (1) detecting and stopping the vehicle and its occupants, (2) performing measurements in the field and (3) the reachback centre analysing the data and returning the results, other actions have to be taken to clarify the issue and the situation. This involves border forces, customs authorities, national authorities, etc.

The actions to be taken when sources are detected are outlined below.

- If there is no threat or no hazard other than radiation, this is dealt with as a regular sanitary issue and the relevant agency sends a specialist team to collect the source.
- If a threat is identified, the dedicated French Home Office Unit for Radiological Expertise (Détachement Central Inter-ministériel d'Intervention Technique) will be alerted, sending specified human and material resources to counter the threat. This unit includes several teams from state agencies specialised in the various skills needed: the police and Gendarmerie, the DGA (the French Directorate-General of Armaments), the Laboratoire Central de la Préfecture de Police (LCPP), military explosive ordnance disposal (EOD), civil security organisations and Centre d'Etude Atomiques (CEA) for RN material.

Such an event then has to be declared to the Incident and Trafficking Database of the International Atomic Energy Agency (IAEA).

3.8. Conclusions

An RN exercise, involving several parties including first responders and remote reachback experts, was held at a French border post. It involved a real gamma-emitting source and the French reachback expertise centre, the CNER, played a 'triage' role by analysing data from the field for validation and, at the same time, offered support on radiological matters to the in-the-field actors at various stages of the operation.

The CEA is involved not only during exercises, but also in several steps before and after, giving advice on detectors, courses and training, procedures, etc., and of course giving support in the event of real cases, which happen regularly (the cases of a contaminated candlestick in a container and an empty bottle with a 'uranium' label, to mention some).

This exercise demonstrates how to handle the trafficking of MORC at a border crossing, with means that are appropriate for responding to such a threat. For any country wanting to obtain a reachback capability, the solution could be adapted and applied as below.

- The first responder team involved could include first responders other than fire officers. The most important things are the nature of the training of the first responders and that joint procedures have been established with other parties.
- The means could be less sophisticated, starting with inexpensive detection systems, at least one RPM and one handheld detector with identification capabilities.
- The same applies for reachback capabilities, with at least one RN expert and appropriate software or tools for data analysis (gamma spectra analysis) being required.

The detection of illicit trafficking is an achievable goal with the right means. Since the real issue starts only after first-level detection, it is necessary to prepare and test the whole detection architecture, which includes both human and material means. Learning and training are the key elements of success.

4. Reachback demonstration: Magic Maggiore

H. Tagziria, JRC, Italy

Abstract

This chapter describes a demonstration exercise of an incident at a border crossing involving the illicit trafficking of special nuclear material masked within fertilisers. The demonstration primarily focused on the reachback that followed, its main components of alarm adjudication, detection technologies and their capabilities, as well as on the information exchange between FLOs at the border crossing, a national reachback centre (NRC) and an advanced reachback centre (ARC) in another country. All three sites were connected via live web streaming to the auditorium.

4.1. Introduction

The European Commission's Joint Research Centre (JRC) in collaboration with the Global Initiative to Combat Nuclear Terrorism (GICNT) developed and organised the [Magic Maggiore Technical Reachback Workshop](#), held from 28 to 30 March 2017 in Ispra, Italy, which was attended by more than 65 technical, scientific and operational experts in the area of technical reachback from more than 25 countries.

The workshop aimed to raise awareness and make the first steps towards a commitment to technical reachback and its main pillars, promote the exchange and sharing of best practices, and promote models to address important operational, technical and organisational challenges.

To reach these objectives, obtain key findings and identify future work areas and gaps, the workshop was organised around presentation lectures, panel discussions and a real-time demonstration of the detection of illicit trafficking at a border crossing and the reachback that followed during the investigation. The workshop was essentially structured into four sessions covering (1) the role of scientific and technical expert support, (2) the opportunities and challenges of technical reachback (including a demonstration), (3) how to build on the core components of technical reachback and finally (4) advanced technologies.

The demonstration was developed and organised by the JRC in Ispra in collaboration with the French Centre d'Etude Atomiques (CEA) and members of the Thematic Group for Radiological and Nuclear Threats to Critical Infrastructure (the ERNCIP RN Thematic Group). The event focused on the main components of alarm adjudication and detection technologies and their capabilities, as well as on the information exchange between FLOs at the border crossing, an NRC situated (in this scenario) at the JRC in Ispra and an ARC effectively situated in France.

This chapter aims to describe the demonstration scenario and its main findings and conclusions.

4.2. Objectives of the demonstration

The demonstration aimed to raise awareness of the various reachback roles and the support available to FLOs, and best practices for information sharing. The detection

scenario was developed to serve as a platform to illustrate initial data acquisition procedures and the difficulties faced by FLOs in alarm adjudication due to a number of issues, including organisational and technological (e.g. low energy resolution detectors) issues and those related to training and expertise. The demonstration then evolved to show the interactions between the FLOs and reachback centres with a focus on data acquisition, transfer and interpretation. A mobile expert support team (MEST) or expert team provided additional identification tools, demonstrating the excellent performance of high-resolution spectrometric equipment. The demonstration also addressed operational problems due to the lack of compatibility of legacy equipment with state-of-the-art equipment and the poor standardisation of structures and protocols for spectral data exchange at national and international levels. The definition of relevant data to be shared, data structures, alarm notification procedures (databases) and the role of international organisations were discussed, as well as the need for bilateral or multilateral reachback agreements. The audience was invited to participate in a closing discussion to further define the roles of reachback support and the optimisation of resources.

More specifically, the demonstration aimed to illustrate the need for expert knowledge for the correct interpretation of spectra, including:

- the importance of the proper identification of the radioactive and nuclear materials (category, isotopic content);
- the relevance of safety assessments (local protection) and security/non-proliferation assessment;
- the advice regarding material isolation, shielding, masking, transport and storage;
- the necessity to proceed properly during detection and onsite response for later forensics, respecting established and agreed standard operating procedures (SOPs) and CONOPs.

At the reachback centre in the large auditorium, discussions took place regarding the energy resolution of spectra, the decision mechanism, communication protocols and the scalability of FLO tools, capacity, capability building, and cooperation and communication between competent authorities.

4.3. The demonstration scenario and actors

As illustrated by Figure 4.1, the scenario involved:

1. a border crossing situated at the JRC, Ispra;
2. the NRC, situated in the auditorium of JRC, Ispra, with a streaming video link to the border crossing;
3. the ARC, situated at the CEA in Paris with an authorised streaming video link to JRC, Ispra;
4. the audience in the auditorium (streaming video link to the event scene), who could:
 - a. observe the detection team and the technical reachback team
 - b. observe the interactions between both teams
 - c. discuss the ongoing event;
5. national competent authorities, with which to liaise to authorise a plan of action.

Video cameras were set up at the border crossing to record and web stream the event in real time to the auditorium. Similarly, cameras were also set up in France with a secure and authorised internet link to JRC, Ispra.

THE SCENE

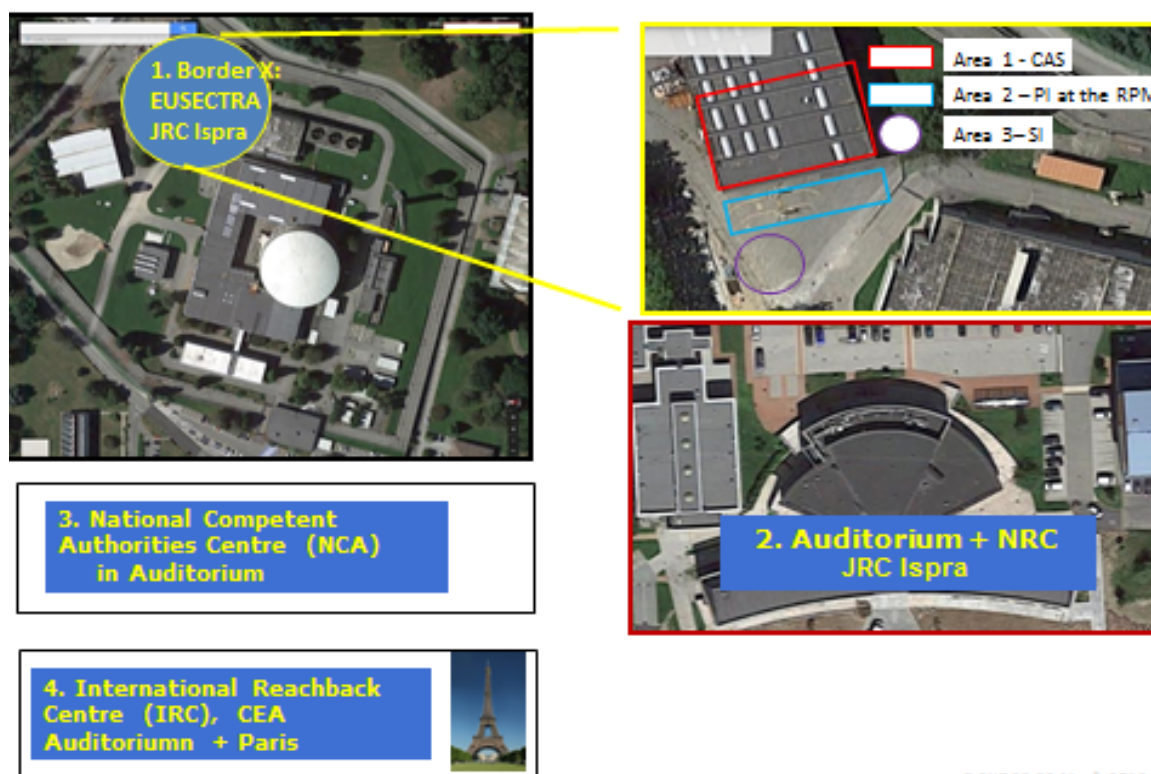


Figure 4.1. The demonstration's scenes.

4.4. The scenario in four parts

4.4.1. Part I

A van approaching a border crossing point equipped with a (non-spectroscopic) RPM triggers a gamma-ray-only alarm, which led the officer to take the van aside to check documentation, question and observe the driver, and proceed with a secondary inspection. A legal transport of fertilisers is declared. Inside the central alarm station (CAS), other experts proceed to examine the RPM report and the profile of the radiation detected. Based on past experience and knowledge, the CAS recognises an unusual profile that is not compatible with fertilisers. Furthermore, the FLO that approaches the vehicle with a personal radiation detector finds a radiation hotspot at the back of the van. He first checks that dose rates are safe (below 100 $\mu\text{Sv/hr}$ at 1 m) and performs a quick measurement for identification using a standard RID. The results are inconclusive as regards the identification of the material. The FLO team leader therefore decides to seek help from the NRC, in accordance with SOPs and CONOPs.



Figure 4.2. The scene at the border crossing including CAS and video streaming setup.

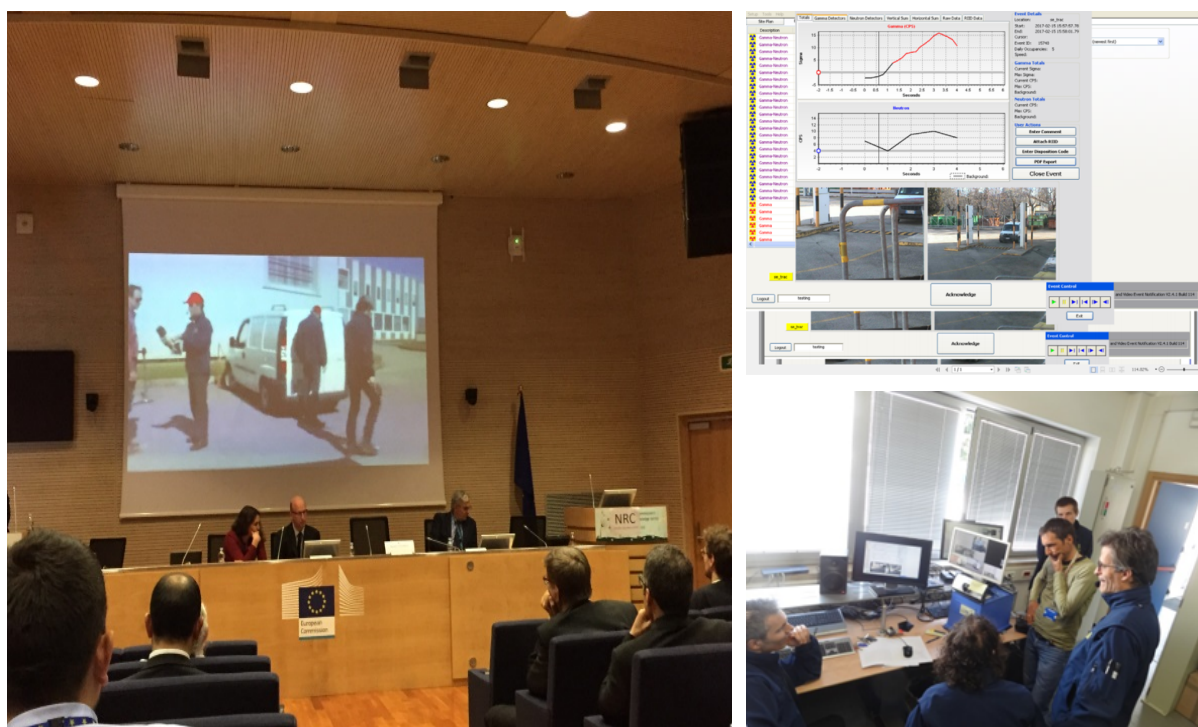


Figure 4.3. The secondary inspection being performed at the border being web streamed to the auditorium and FLO team discussing the incident and the radiation profiles in the CAS.

4.4.2. Part II

On the telephone, as captured by the video cameras, the FLO team leader at the border crossing is heard summarising the situation described above in Part I to the NRC focal point who requests further information such as the dose rate at 1 m, identification results, what instruments were used, whether or not they were calibrated, whether gamma-only or gamma-neutron radiation was detected, what the measurement time was, etc. Some equipment does not have the capability of transmitting data remotely, while some do, but the transmission format shows variations that make communication and analysis complicated. The FLO team leader sends screenshots of the RPM profile and energy distribution spectra, as well as a template completed with relevant information and the information requested, including:

1. event description
2. spectra:
 - a. unknown item
 - b. background
 - c. known source
3. distance between detector and item
4. time of collection
5. type and mode of detector
6. neutron count rates
7. dose (although this can be deduced from spectra)
8. shielding
9. photos
10. isotopes identified
11. contact name and telephone number.

Having analysed all data and information, the NRC instructs the border FLO team to temporarily hold the van and deploys an expert to the site with high-resolution gamma spectrometers.

4.4.3. Part III

The NRC expert arrives onsite to make the standard 300 s long measurements with high-resolution equipment, report to the national focal point and send spectral data, screenshots and the identification results to the NRC headquarters. Once all data are analysed and discussed, the NRC team decides that this is a serious incident that presents technical challenges and difficulties beyond their capabilities and that help is needed. Consequently, a call is made to brief the national competent authorities on the situation and to request an authorisation to call the ARC and share the data as per the bilateral agreement and protocol previously established. The authorisation is granted thus allowing the transmission to the ARC of the data and information obtained so far, including the inspection report, identification results, raw spectra and dose rates. The audience in the auditorium follows all these interactions via live web streaming. The ARC (in Paris) interacts with the NRC and analyses the available data. Once the analysis is complete, a confidential report is sent to the NRC confirming that a serious incident involving the presence of weapon-grade plutonium masked within fertilisers has occurred.

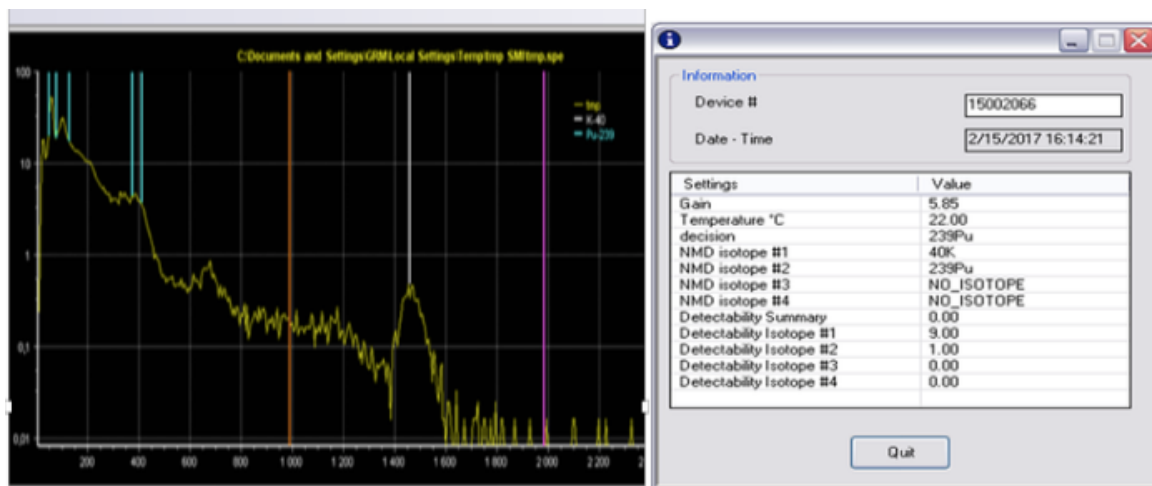


Figure 4.4. Identification with high-resolution RID and spectrometer.



Figure 4.5. Gamma-ray energy spectra transmitted and being analysed by the ARC.

4.4.4. Part IV

The NRC notifies the competent authorities, who decide to launch a national response plan with two options addressed and discussed by the audience as outlined below.

Option 1:

- the vehicle is moved to a secured and controlled area making sure evidence is preserved;
- the driver is placed in custody by the competent authority;
- forensics are performed;
- prosecution, etc., follows.

Option 2:

- vehicle and driver released and followed to gather further intelligence and maximise outcome.

A discussion is opened in the auditorium following a summary of the demonstration and its challenges are revisited with the audience.

4.5. Conclusions

The interactive demonstration and the discussions that followed underlined:

- the importance of alarm adjudication and information-sharing processes as well as detection technologies in ensuring an appropriate and effective response;
- the importance of adequate and sustainable training of FLOs and the technological tools at their disposal for effective alarm adjudication and reachback;
- the importance of considering legacy equipment, detection equipment and varying levels of capabilities and preparedness within a country and internationally;
- the importance of having established and agreed SOPs and CONOPs, as well as bilateral or multilateral agreements and protocols with third parties and expert centres (national or international), to ensure effective reachback and an effective nuclear detection architecture;
- the need to continually review and update all aspects of the processes of the NSDA based on new threats and risks, experiences (including demonstrations and exercises), new information and capabilities.

The Magic Maggiore workshop demonstration and exercise focused on a number of important and challenging issues. The demonstration raised awareness among the audience regarding the need to establish technical reachback. It illustrated important aspects of best practices in ensuring a sound NSDA and addressed some of the key challenges and knowledge gaps identified during the workshop.

5. REPO technology and the Estonia-Finland cross-border reachback demonstration

K. Peräjärvi¹ and J. Raidloo²

¹STUK (Radiation and Nuclear Safety Authority), Finland

²Estonian Rescue Board, Estonia

Abstract

Responsibilities related to nuclear security detection activities are typically divided among several government organisations. To have an efficient and cost-effective NSDA, the relevant organisations need to cooperate. Information sharing is the key to success. Organisations must be able to efficiently share technical information. This case study examines the role of technical, scientific and operational remote expert support, i.e. reachback. It also investigates the added value of cross-border reachback support and introduces the outcomes of the REPO (RElocatable PORTal monitor) project.

5.1. Introduction

In this paper, the term 'reachback' means remote expert support. In Finland, three different modes of reachback are utilised: (1) technical, (2) scientific and (3) operational reachback. Technical reachback covers on-call remote assistance for FLOs in matters of technical detection instruments. Scientific reachback covers on-call analysis services for FLOs. Operational reachback deals with the real-time technical and scientific support for FLOs and MESTs during special operations.

Figure 5.1 presents a typical data processing diagram illustrating the stages of a nuclear security event and the terms used. It assumes a situation where layers other than the FLO layer have been activated. The process presented begins from the alarm generated by an FLO's radiation detector. Nowadays, more and more gamma-ray spectrometers are employed in nuclear security (both in primary and in secondary inspections). A gamma-ray spectrometer is a useful instrument, since in addition to radiation detection it may allow the stand-off identification and characterisation of the radiation source in question. The task of the RN specialist who receives the information is first to verify the results of the automatic analysis routines. The specialist should also continue the analysis and finally articulate the RN threat associated with the case. (It may be useful to consider this requirement when contemplating the core reachback capabilities.) RN specialists should acknowledge the potential presence of other threats but if not trained they should refrain from making any conclusions about them. RN experts pass on their findings to the operation centre. The operation centre collects all available information and decides on further actions and communicates them to the reachback centre and the FLOs. In this way, all the actors are kept up to date. Figure 5.1 also includes the possibility to request a second, independent opinion about the data collected. Such a second opinion could be used to reduce uncertainty related to the interpretation of the data collected. It should be noted that official mechanisms for requesting and receiving domestic and/or external expert assistance should be in place and practised before an event. Such mechanisms do not exist between Estonia and Finland and the event presented here was simply a technology demonstration. It is important to develop domestic capabilities even if external assistance mechanisms are available. Joint formats and protocols play a key role.

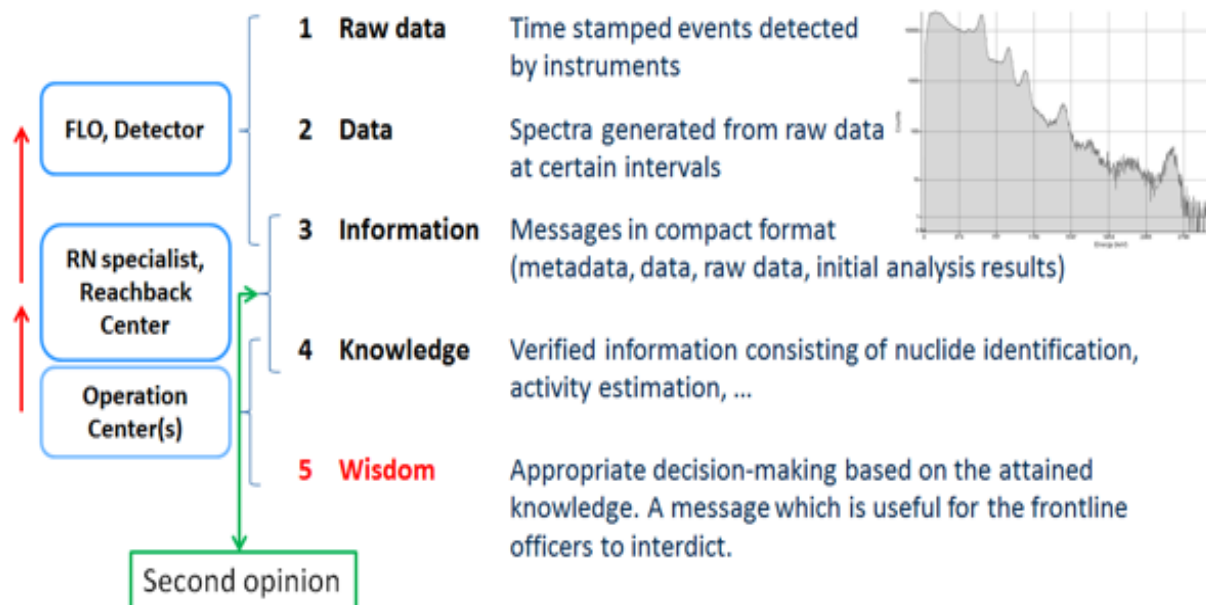
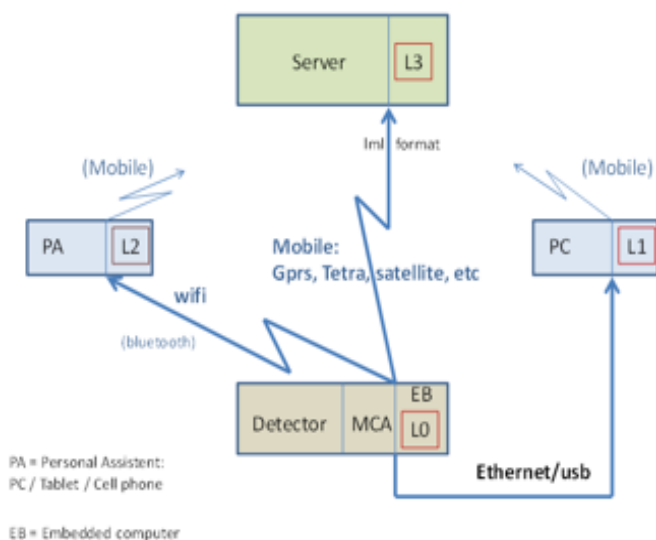


Figure 5.1. Process from 'raw data' to 'wisdom'. The aim is the efficient use of data.

5.1.1. REPO project 2012-16

The REPO project was coordinated by the Radiation and Nuclear Safety Authority, Finland (STUK). It was partly funded by TEKES, the Finnish Funding Agency for Innovation. The project was split into two parts. In the first part, 2012-13, the first Finnish NSDA was developed. Moreover, several technologies were identified for further development by companies. During the second phase, 2014-16, companies developed these technologies and demonstrated their use in practice. The technology demonstrations delivered by these companies were evaluated by the participating government experts. The findings were communicated back to the companies. From the authority side, this iterative process ended with the development of procurement specifications, i.e. the REPO project did not include the actual purchase of equipment. Obviously, the procurement specifications developed were used by the authorities later on. The main requirement for REPO detection equipment is that it must be able to store the data collected in a remote database that is accessible by RN experts (see Figure 5.2). In addition to detection instruments, the REPO project companies also developed software tools for secure data transfer and real-time monitoring. During the REPO project, it was not possible to organise a large-scale demonstration to examine the mixed use of companies' and authorities' soft- and hardware systems.

Detection system, including LINSSI databases (L0-L3)



Applications:

1. Relocatable detectors
2. Hand-held detectors
3. Backpacks
4. Car, ship, UAS
5. Other (metal industry)



Figure 5.2. Schematic drawing of a REPO detector that is also capable of storing data in a remote database. The REPO project device shown at the bottom right is one example of such a detector.

5.2. Estonia-Finland cross-border reachback demonstration

Reachback is an important cross-cutting theme in the domestic part of the Finnish NSDA. The Finnish NSDA also takes part in bilateral, regional and international collaborations. Investigating the usefulness and feasibility of reachback in bilateral cooperation was a partial driver behind the Estonia-Finland cross-border demonstration. The demonstration also gave Finnish authorities an excellent opportunity to comprehensively test the REPO technology developed. Cross-border technical and scientific expert support is also addressed in the 2017 European Commission action plan on CBRNE security risks. This was the main reason why the JRC/Thematic Group for Radiological and Nuclear Threats to Critical Infrastructure (the ERNCIP RN Thematic Group) decided to produce this document.

The date of the demonstration was 22 November 2017. The demonstration was based on a scenario where Finland sent to Estonia a multidisciplinary team consisting of authorities and radiation detection experts from the private sector to stop the attempted illicit trafficking of radioactive material in Tallinn. The field team and operational reachback centre were based in Tallinn and on-call scientific support in Helsinki. The Estonian Rescue Board was the host organisation and also led the operational reachback centre. Private Finnish companies, which were part of the REPO project, performed the practical detection work in Estonia. The Finnish Radiation and Nuclear Safety Authority, STUK, provided optional on-call scientific support.

A 2" × 2" LaBr₃ gamma-ray spectrometer was employed as a backpack detector. Information on the location of the backpack detector was determined using an integrated global positioning system (GPS) unit. When switched on, the backpack detector first calibrates itself and then starts to make short-term measurements (typically 4 s). The

detector is automatically gain stabilised. Recorded data are stored in real time both locally and in the remote Linssi database. Both the operational reachback centre in Tallinn and the on-call scientific reachback centre at STUK were granted access to this remote database. In practice, this meant that STUK could also monitor the progress of the field measurements in real time.

At 10.41 a.m. Coordinated Universal Time (UTC), the operational reachback centre contacted STUK. The field mission was about to begin in Tallinn and STUK was requested to get ready in case needed. Online monitoring of the field mission by STUK was not requested. After the call, a scientific reachback centre at STUK was activated. It should be noted that the expert support required can be located almost anywhere, since only access to the internet is required. This provides a lot of flexibility for organising reachback support outside office hours. Quite soon after starting the radiation surveillance mission, an instrument alarm was triggered. The automatic analysis algorithms identified Co-60. This information was verified by the operational reachback centre in Tallinn. A second opinion from STUK was not needed.

The second instrument alarm was triggered around 10.59 a.m. UTC. The automatic analysis algorithms identified Co-60 and Am-241 (see Figure 5.3). Since multiple nuclides were detected, the operational reachback centre decided to request a secondary analysis from STUK in this case.

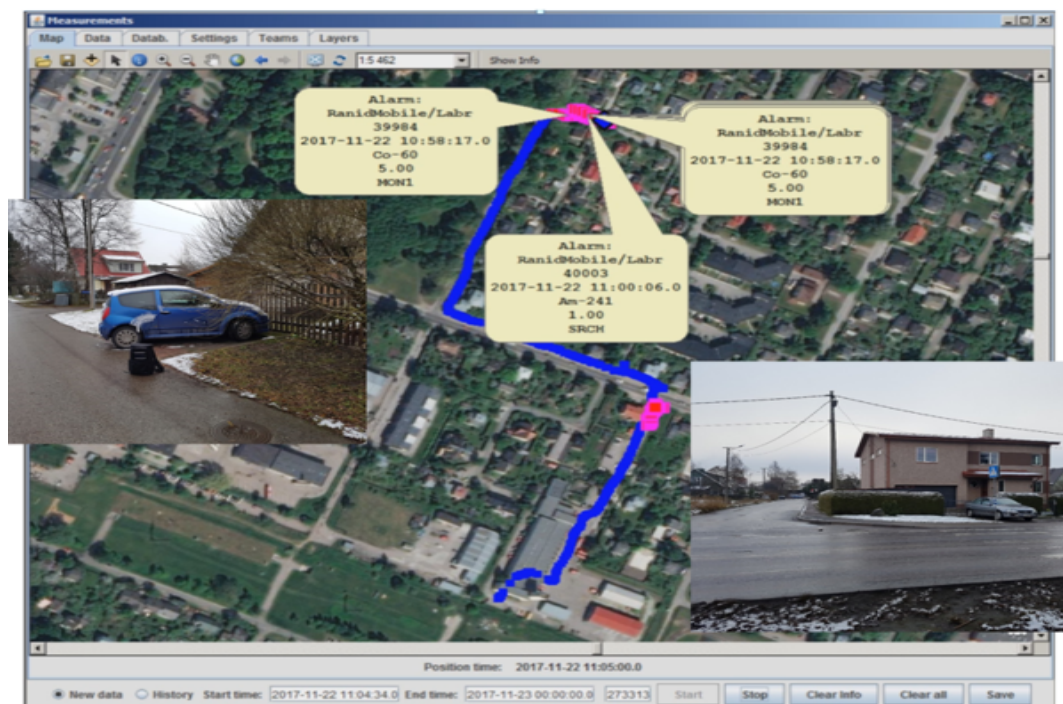


Figure 5.3. Patrol movements displayed on a map. The path taken during the field mission is indicated by the blue line. Alarms are marked with red/pink colour. The automatic analysis algorithms identified Co-60 and Am-241 nuclides. In addition, the photographs from the alarm sites were submitted into the reachback system of STUK. Selected gamma-ray spectra are analysed using different software. Similar views of the scene and similar data were available at the operational reachback centre in Tallinn.

The maximum gamma dose rate associated with the second instrument alarm was about 2 $\mu\text{Sv/h}$. The sources that triggered the second instrument alarm were localised in a car, as shown in the photograph on the left in Figure 5.3. The backpack detector used is visible in the front of the car. (In reality, for safety reasons, small calibration sources were

employed in the demonstration and placed next to the detector only when needed.) To allow more detailed analysis, multiple 4 s spectra were summed.

Rapid manual spectrum analysis was done using separate software. The analysis confirmed the presence of Co-60 and Am-241. In addition, Cs-137 was also detected. By analysing different spectral features, it was concluded that the sources were not shielded. After combining all available information, it was concluded that the RN threat was rather low. These results were communicated back to the operational reachback centre in Tallinn. Similar conclusions were independently made there. The overlap of the expert opinions added confidence and simplified the work of the decision-makers. It should be noted that this analysis deals only with the RN threat, i.e. the presence and significance of other threats need to be considered separately.

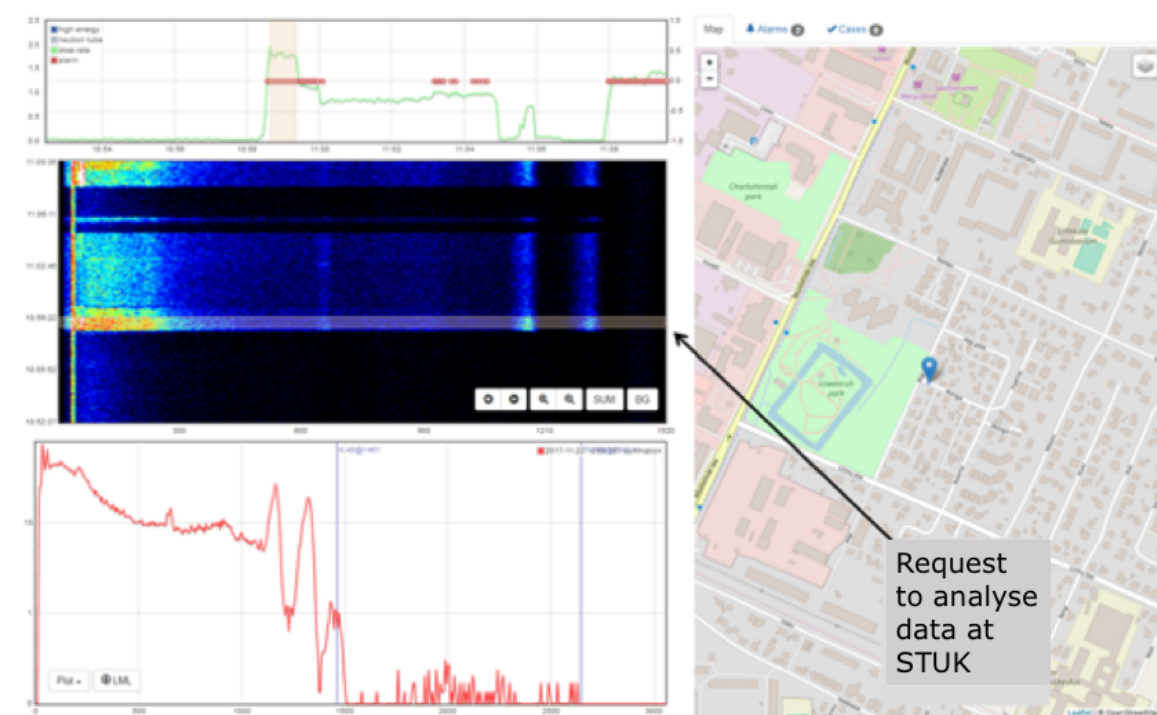


Figure 5.4. Various depictions of the data collected. Top left: changes in dose rate and generated automatic alarms (red circles) over time. Middle left: gamma-ray spectra collected in waterfall format, with time on the vertical axis and gamma-ray energy on the horizontal axis; each line in the plot corresponds to one 4 s spectrum; the warmer the pixel colour the more counts were detected with that energy and time. Bottom left: a window for individual gamma-ray spectrum and summed gamma-ray spectra.

5.3. Conclusions

The REPO technology that had been developed functioned well. The mixed use of authority analysis systems and commercial measurement services was possible. Joint formats and protocols were employed. In the demonstration, all information collected was also accessible to STUK. If countries find it hard to share all information during a mission, one option would be to share a single spectrum with the minimum amount of metadata needed for the successful RN analysis of data. Downgrading from full operational reachback mode is easy. This demonstration introduces only one potential scenarios in which countries may consider sharing technical information. Mechanisms for requesting and receiving technical assistance should be in place and practised before an event takes place.

6. Exercises and testing nuclear detection capabilities using an electronic platform

H. Toivonen¹ and S. Ihantola²

¹HT Nuclear Ltd, Finland, ²Radis Technologies Ltd, Finland

Abstract

A simulation tool, known as Thimulator, is introduced. The software has two main applications: (1) to be used as a platform for realistic tabletop exercises and (2) to test the capability of measurement technologies for providing radiological information in a timely manner. Thimulator software executes a field mission virtually, sending the instrument data to the reachback centre in real time. The software simulates the movements of various measurement systems, such as a backpack or vehicle patrol or unmanned aerial vehicle, and provides data to experts to be analysed and transmitted to the operative units and decision-makers.

6.1. Introduction

Information sharing is key to responding efficiently to nuclear security events and emergencies. Information needs to be shared at national level between various authorities and, in the case of large-scale events, also internationally, to obtain support from other countries. The Thematic Group for Radiological and Nuclear Threats to Critical Infrastructure (ERNICIP RN Thematic Group) has identified a potential approach for improving data exchange at the technical level, which is outlined in the report *Remote expert support of field teams – reachback services for nuclear security* [6.1].

The report proposes the development of joint formats and protocols based on existing data structures and open-source databases, whereby each instrument or user can communicate with other relevant users.

The advantages of seamless information sharing in various threat scenarios can be tested with the simulation software presented in this paper. The software simulates the radiation field where the users of the software can freely move various detection systems. On one hand, this enables the capability of the chosen detection method to be tested as a component of an NSDA. On the other hand, the digital platform is ideal for training and exercises because it can be safely used to simulate realistic threat scenarios.

The simulations provide radiological data based on the chosen instrument and geolocation. Each user can independently perform their own field work or data analysis and receive information as it happens in reality. The virtual world is ideal for testing nuclear response capabilities; it paves the way for identifying efficient means of handling nuclear threats.

The present paper describes an example scenario, namely a search operation to find radioactive MORC. The scenario involves a simulated vehicle equipped with a gamma-ray spectrometer. The users see the operation as they would if they were in the reachback centre supporting a field mission, that is, the vehicle is monitored and shown on a digital map with realistic radiological data that would be used for analysis and decision-making.

6.2. Simulation of threat scenarios

The simulation software, known as Thimulator (a threat simulator, HT Nuclear Ltd, Finland), was designed for assessing the capability of detection instruments in field conditions and for training and exercises. On a digital platform, users can plan and perform prevention, detection and response measures at borders or in interior parts of a country [6.2].

RN threats vary widely. The event may be an accident or intentional. The criminal or unauthorised use of radiation may take different forms, depending on tactics, the material and the target. Thimulator is designed to handle different radiological scenarios, from illicit trafficking and contamination to nuclear fallout.

Through simulation, a tailored scenario is run in real time. The scenario can take place anywhere in the world. The cooperation of operative units with nuclear experts is tested in a time-critical event. Users can choose from various detection instruments, such as dose-rate metres and spectrometers (hand-held or backpack), and patrols may move using vans or any other means of transport. In addition, field teams are supported by nuclear experts (in a reachback centre). The analysis results provided by Thimulator can be used for advice and for planning countermeasures.

Thimulator helps to test the suitability of various detection systems and strategies in a variety of scenarios. A digital mapping environment is used to define the movement of the field team. During the simulation, the team receives radiological information based on their geographical position and the chosen detection instrument. The movements of the field units are displayed in real time using [OpenStreetMap](#) [6.3].

In addition to testing and optimisation, Thimulator can also be used as a digital training platform to create an electronic tabletop exercises (eTTXs). In an eTTX, participants work with personal computers linked to a server that provides radiological information services on digital maps or in other formats, such as reports, as a function of time. The mission can be followed in real time, paused or accelerated by a factor implemented by the exercise organisers. In an eTTX, the radiological information has to be acquired realistically by moving first responders to the threat area, and the value of the information gathered will be assessed by nuclear experts.

6.3. Search for radioactive material in a virtual world

The following example demonstrates the search for MORC using a van equipped with a gamma spectrometer (Figures 6.1 and 6.2). The operation may be part of a larger illicit trafficking event involving the acquisition of radioactive material to attack civilians in a major public event (MPE). The authorities have received information alerts and are able to narrow the search operation to a certain industrial part of a city. The aim of the scenario is to illustrate how the participants use Thimulator to acquire and process information in the search operation for the incident commander. The timeliness of the search operation, including digital information sharing and voice communication, is of high importance.

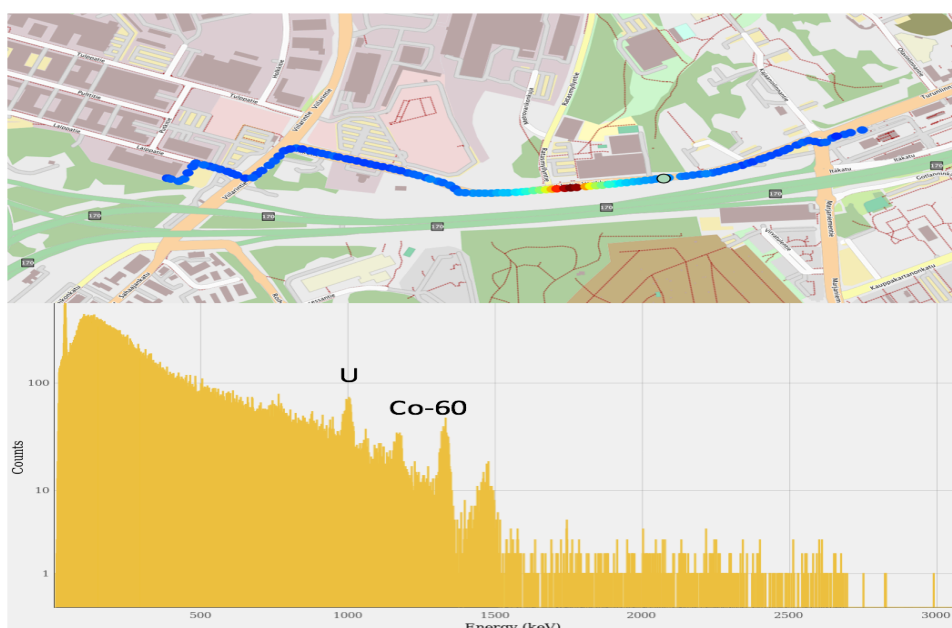


Figure 6.1. Search operation for radioactive material with a spectrometer installed in a van. The movement of the van is followed on a digital map in real time. At a certain location, the count rate is greatly elevated indicating the presence of a possible source. The spectrum reveals that the source contains Co-60 and uranium. The spectrum is interpreted by a nuclear expert: the source is thought to be heavily shielded because the 1 332 keV peak of Co-60 is much larger than the 1 173 keV peak. The presence of uranium could be explained by a depleted uranium (DU) shield.

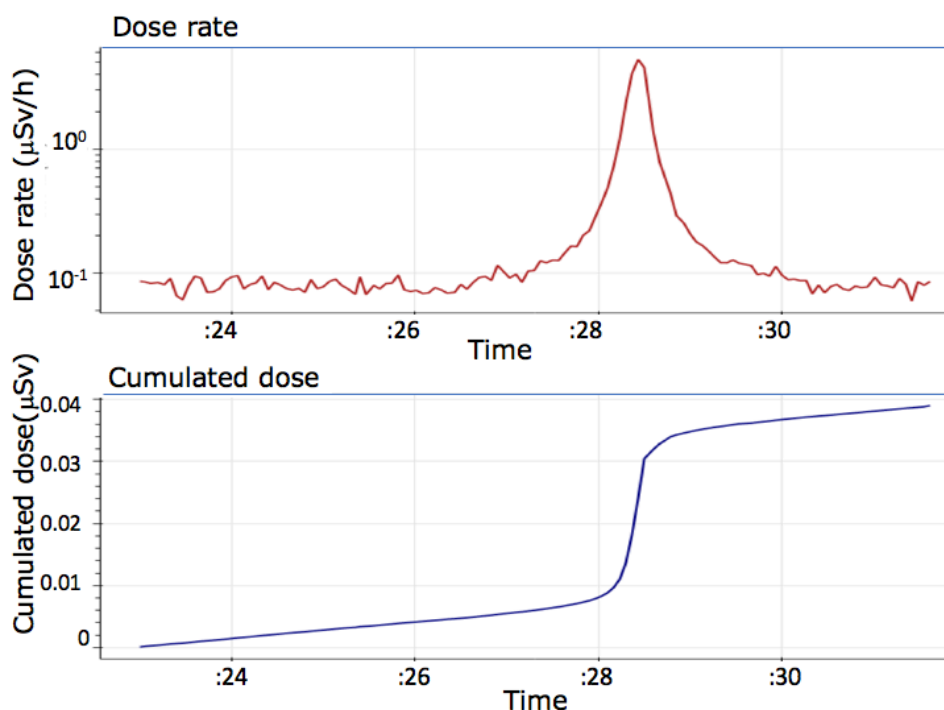


Figure 6.2. Dose rate while passing the source in a van (at a speed of 20 km/h) and the integrated dose received by the staff inside the van. Time is given in units of minutes since starting the mission.

The participants are tasked to evaluate the mission from the point of view of timeliness, technical capabilities and the value of the information received. A relevant discussion point is whether all EU Member States should have this kind of advanced mobile detection asset or whether there should be international arrangements in place to ensure help can be rapidly obtained from other Member States or international organisations.

The data in Figures 6.1 and 6.2 contain many important pieces of information that have to be passed to the response forces for the neutralisation of the threat, including security and safety issues. The critical information is acquired in a few minutes, while the van is passing the source. However, the spectrometric data are complex and require analysis by nuclear experts. There must be efficient communication links in place combined with advanced data management capabilities, including automated analysis processes that provide the first view for the analysts located in a remote expert support centre. The process is triggered by an instrument alarm that must be transmitted not only to the crew of the van but also to the nuclear experts. The measurements reveal the following information, which the analyst should pass quickly to the response forces.

- A radioactive source is detected in a certain location with coordinates (latitude (LAT), longitude (LON)).
- The source is Co-60 and it is heavily shielded.
- The shield is most likely DU.
- The dose rate is about 5 $\mu\text{Sv/h}$ on the road near the location. It is expected that near the source the radiation exposure will greatly exceed 100 $\mu\text{Sv/h}$ requiring immediate safety measures (cordoning, evacuation).
- The source is located near the road ($> 10\text{ m}$); this is revealed by the narrow dose rate pattern in Figure 6.2.
- The activity is unknown, thus requiring further analyses. However, the source is dangerous, probably of the order of TBq.

The information above is of a scientific and technical nature. The findings must be converted to actions that are intended to protect people and simultaneously facilitate investigations at the crime scene. The incident commander and the experts should communicate in detail to plan and execute the next countermeasures without any significant delay.

6.4. Discussion

Efficient information sharing within and between competent authorities is key to the success of countering nuclear threats. On the other hand, the information must be well protected, but not over protected. Initially, the information may be highly classified but at a later stage its security status may change and then it should be distributed rapidly to all relevant stakeholders.

Scenarios implemented in an electronic environment are excellent tools for understanding the information flow, including timeliness requirements. In an eTTX, participants have to estimate how long it would take to initiate a particular detection effort. The software then executes it at a realistic tempo, or at least provides information on how long the field mission will take to implement. The data then have to be interpreted by nuclear experts

and transformed into a format that is useful for the incident commander. This process can show whether or not a particular field mission will give useful information for decision-making in a timely manner. Virtual implementation is much easier, safer and cheaper than a real field mission with relevant threat materials.

The present scenario and related analysis in a modern digital environment show that critical radiological information can be rapidly acquired and shared between participants. Having the same information-sharing capability in the real world requires standardised formats and protocols, compatible reporting from the instruments, and reliable, fast and secure communication at national and international levels. It is possible to deliver scientific, technical and operational expert support nationally and internationally. However, this kind of cooperation requires bilateral or international protocols and agreements. These measures are political and administrative and they should be established during the process of building an NSDA, well before any real incident takes place.

6.5. References

- [6.1] Toivonen, H., Reppenhagen Grim, P., Tengblad, O., Keightly, J., Paepen, J., Abbas, K., Schneider, F., Nilsson, J., Perejärvi, K., *Remote expert support of field teams — reachback services for nuclear security*, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen (ERNCIP), 2014.
<https://erncip-project.jrc.ec.europa.eu/downloads>
- [6.2] Toivonen, H. and Ihantola, L. 'Scenario-based learning to manage nuclear threats in virtual electronic environment', International Conference on the Security of Radioactive Material: The Way Forward for Prevention and Detection, 3-7 December 2018, Vienna, IAEA.
- [6.3] OpenStreetMap
<https://www.openstreetmap.org/#map=7/40.007/-2.488>

7. National and international cooperation — role of expert support

Every NSDA requires close cooperation between competent authorities, including expert support, as a cross-cutting element of the detection architecture, to handle complex nuclear and radiological information of a technical and scientific nature. There are several ways in which this support can be implemented. The IAEA has identified the following prerequisites ([Nuclear Security Series No 15](#) (NSS 15), paragraph 3.14) [7.1]:

- 'Encourage the timely sharing of operational information among competent authorities within the State;'
- 'Ensure appropriate coordination and cooperation with relevant authorities in other States and international organizations'.

The case studies and scenarios discussed in chapters 2 to 6 show that expert support can be implemented in various ways, taking into account the overall goals and implementation strategy of a national NSDA. The following discussion highlights important items for successful cooperation — nationally and internationally.

7.1. Information sharing

Information sharing is crucial for an effective and timely response to nuclear security events. There are two main information mechanisms:

- vertical (the transfer of information along the chain of command, for instance direct instructions from police command);
- horizontal (the transfer of information, in particular technical information, between experts from different authorities).

Both mechanisms are vital. For situations requiring reachback support, the horizontal transfer of technical information is of particular interest. The case studies and the scenarios clearly show the following challenges, which can be national, bilateral or international, depending on the deployment situation: overcoming the communication barrier between different competent authorities; increasing knowledge of the capabilities of the different partners; establishing and testing joint protocols and procedures; and the transfer of restricted information and suitable data formats for the transfer of real-time and spectral data.

An effective way to overcome the communication barrier between competent authorities is to set up face-to-face meetings between the experts who would be required to work together to respond to nuclear security events in an informal setting, for instance during joint training sessions or exercises. This is particularly relevant for experts from radiation protection authorities and the police, because, in general, police authorities and radiation protection authorities have very different institutional work cultures. Such face-to-face meetings will contribute to increasing knowledge about the capabilities of other institutions, but nothing can substitute for intensive joint exercise and training sessions that are extensively evaluated to obtain knowledge about the strengths and weaknesses of interagency responses to nuclear security events.

Ideally, all the required information channels and procedures should be established in operation protocols that have been tested (and adjusted) accordingly during exercises before a nuclear security incident occurs. This can only be achieved with support of high-level government agencies, as it involves organisation, additional training and exercises that require a long-term commitment of personnel. The case studies and scenarios have shown that, an event that occurs in one state, it could involve other states as well. For this reason, high-level agreement is necessary between states to allow the horizontal exchange

of information during a nuclear security event (see, for instance, the exercise scenario involving Estonia and Finland described in Chapter 5).

The transfer of restricted information is an important topic and should be addressed in the operation protocols at national and international levels, especially as information alerts during nuclear security events may be restricted or confidential. It could be advantageous to consider not restricting the real-time measurement data and spectral data collected during a nuclear security event, as this could vastly increase the available data transfer options. One option could be to not restrict the raw data, but to restrict the conclusions of the reachback team.

Finally, suitable data formats for the transfer of real-time and spectral data are needed. This is of utmost importance, so that the data can be read and analysed by the reachback team. It has been shown that a second opinion is a good way of increasing confidence in the conclusions of the reachback team, for instance by using the reachback capability of a different state. For this to work, standardised formats and protocols, such as [ANSI/IEC.N42.42](#) [7.2], should be agreed upon before a nuclear security event occurs. Mechanisms for requesting and receiving assistance should be in place and practised before the event.

7.2. Political-level agreements and cooperation between states

National-level RN strategies and detection architectures should recognise the importance of cooperation with other states. International threats connected to RN materials need to be taken sufficiently into account. Information exchange helps with long-term risk analysis and response development. Cooperation during serious nuclear security incidents should also be considered. Information sharing does not have to be comprehensive or complete, if states would find this too difficult. Sometimes, sharing only a single spectrum with a minimum amount of metadata may be sufficient for successful RN analysis. Downgrading from full operational reachback mode is technically simple.

Joint cross-border operational capabilities require continuous training and exercise programmes. If states have similar needs, they could also cooperate in their technical capacity development. Since serious nuclear security events are rare, it could be considered that not all states need to own and maintain all possible state-of-the-art detection capabilities, such as systems for the monitoring of large areas for airborne fallout. Instead, there could be political agreements in place so that such capabilities could be rapidly obtained from other countries, if and when needed. The same also applies to advanced nuclear forensics capabilities.

7.3. CONOPs and expert support in nuclear security

Detection systems and the related information management are often designed for the control of state borders. Another approach is to focus on the interior layer of the state (MPes, critical venues or traffic nodes, such as railway stations). To achieve the nuclear security goals of a state, a CONOP should be developed defining clear roles and responsibilities for each competent authority. A CONOP should deal with the requirements of different detection architectures and different detection systems:

- CONOP A: primary screening with large (plastic) counters followed by secondary screening;
- CONOP B: spectrometric portal monitors;
- CONOP C: mobile instruments.

CONOP A works well for states that can allocate personnel for secondary measurement, although the false alarm rate could be high. CONOP B may be chosen by states that aim to minimise false and innocent alarms at an early stage of detection (to minimise human resources); the implementation of CONOP B requires real-time reachback services, including a high-quality analysis capability and reliable communication links. CONOP C is based on relocatable, wearable, handheld, vehicle-based or other types of mobile detection instruments, which are deployed according to the intelligence information or information alerts. In all cases, well-organised and efficient expert support is required to launch a fast and balanced response when needed.

7.4. Technical tasks for expert support

To ensure the timely sharing of operational information among competent authorities within a state (as stipulated in the IAEA's NSS 15), technical expertise relies heavily on the detection technology available including communication tools and capabilities. However, any detection architecture would fail if it was solely dependent on detection per instrument. Detection based on information, adequately trained and sustained personnel who are well rehearsed in the national response plan and the existing SOPs and CONOPs, and appropriate coordination and cooperation mechanisms are all important building blocks that must be fostered as integral parts of the detection architecture.

There has been good progress in recent years in the field of detection technologies as a result of the drive for research and development (R&D) and innovations in, for instance, He-3 alternatives for all categories of RN detectors, list mode data acquisition, digitisers, GPS and communication capabilities based on Wi-Fi, 3G/4G, Bluetooth, relevant solution software and databases. There has also been a big push for mobile and relocatable systems, backpacks and more recently robot- and drone-ported systems. Terrific, for instance, is an ongoing EU Horizon 2020 project that aims to further develop capabilities for radiation detection with networked unmanned and manned vehicles. Finally, great progress is being made in R&D on gamma-ray and neutron imagers, and there are on the market systems that have demonstrated their potential use in nuclear safeguarding and nuclear security.

Great strides have been made towards the standardisation of data formats. The latest achievement is the development and publication of an International Electrotechnical Commission (IEC) standard on list mode data acquisition ([IEC 63047:2018](#)) [7.3].

The progress made in technology in recent years has made it possible to control and supervise the various detection instruments (RIDs, backpacks, mobile devices) deployed during a mission, including data transmission to a control and command base or reachback centre for data analysis and further processing, for the implementation of countermeasures. The integration of security systems and interoperability between hardware and software is consequently being developed and enhanced. The improved quality of detection technology has been witnessed within [ITRAP±10](#) [7.4] and other EU projects such as [Scintilla](#) [7.5] and [C-BORD](#) [7.6].

States and regions or even organisations within the same state cannot all have the same capabilities, wealth and levels of awareness and preparedness and nuclear security culture, or face the same threat levels. It is noteworthy that no state or organisation would be expected to retire all its legacy equipment in favour of novel technologies with all their advantages and capabilities. Hence, one could advocate a staged approach with perhaps three levels of reachback capability (see Appendix 1) and preparedness that could be enhanced by the sound collaboration and cooperation between regions and states, for

example through bilateral/multilateral agreements and the sharing of training, equipment and facilities. Ultimately, an international reachback centre could be the aim.

7.5. Benefits of reachback

During a nuclear security incident, personnel working at the scene have to fulfil many tasks, for instance ensuring their own safety, making the necessary measurements and advising other personnel about the situation. Using remote expert support reduces the number of tasks that personnel onsite have to complete and simplifies some of the remaining tasks at the scene. This makes the work at the scene less prone to errors and helps to ensure safety.

A reachback centre can access additional information and use sources of information, for instance databases, which are not available at the scene. Nuclear experts can complete time-consuming tasks such as scientific, nuclide-specific calculations or dispersion modelling. Use of this information leads to an improved situation assessment. In addition, reachback can support documentation and ensure completeness and consistency.

A reachback centre should give good advice to command and control, and support the comprehension of the situation that onsite personnel are dealing with. Given the information from onsite personnel, nuclear experts can support the decision to send special equipment or additional personnel to the site.

7.6. Requirements and capabilities of expert support

Expert support, or reachback, is widely acknowledged as a crucial cross-cutting element of an NSDA. The concept itself is poorly defined and understood differently in different states. One possibility would be to distinguish the concepts of expert support and reachback; however, this would have to be agreed at international level. Expert support would have a wider meaning than reachback.

- Reachback could be defined as a virtual network of subject matter experts that provide advisory, technical, scientific and coordination assistance.
- Expert support could include reachback and an operational or technical capability to deploy resources in the field to resolve a potential or actual nuclear security event.

Expert support could also involve informing and advising those in the field, without actually deploying an expert team to the field.

Not only there are conceptual problems, but the reachback capabilities themselves are not defined. The functional capabilities of reachback contain political, legal, administrative, technical, scientific and operational issues. These matters should be clarified and agreed at the international level. The ERNCIP RN Thematic group has made a first attempt to list the items that need to be considered (see Appendix 1).

7.7. Different types of reachback centres

The cases, scenarios and demonstrations presented in this document indicate that there are different types of expert support. Reachback centres can be ranked by their level of capability, both material and human.

Since it is expensive to build a complete structure or architecture (an NSDA) from scratch, starting from a 'basic capabilities level' is recommended (see Appendix 1).

A second level is illustrated by the Finland-Estonia cooperation demonstration (see Chapter 5), where several types of detectors (backpack, handheld) and several experts were involved, both in the field and in an NRC, with real-time data transfer. The BfS case study of a real intervention also involved a whole team, with measurements made in the field and in the laboratory (see Chapter 2). Other capabilities can be included for this level, such as vehicle-borne systems (i.e. detection embedded in a vehicle) or robotic-based systems.

The Magic Maggiore demonstration (Chapter 4) and the cross-border component of the Finland-Estonia cooperation illustrate what could be the third level of expert support: a dedicated team in the reachback centre carrying out several parallel analyses, direct and immediate data transfer from the field, and a multitechnology spectrum analysis capability (including high-resolution spectrometry (HPGe) and neutron measurements). The CEA case study (see Chapter 3) also demonstrates such capabilities, with experts on duty 24/7 and a specialised multisite, multi-expert team. Unmanned aerial vehicles (UAVs) and other aerial means (helicopter, fixed-wing aircraft) can also be included at this level.

Advanced expert support capabilities include calculational means and the modelling of different detection systems and measurement geometries. The implementation is based on specialised algorithms and 'home-made' software, in particular including Monte Carlo calculation and other simulation tools, such as Thimulador (see Chapter 6). Simulations with software such as Monte Carlo N-Particle Transport Code (MCNP) are well suited to approaching the reality of the source, the detector and its environment. At this level, the entire technology, including all types of gamma spectrometry and neutron measurements, list-mode data acquisition (time stamps of events) and possibly other technologies, should be managed by the reachback centre (and, of course, in the field). The different data formats should also be handled without problem, and communication means should be strengthened, with several technology solutions and backup systems, such as communication via satellite.

7.8. References

- [7.1] IAEA, 'Nuclear security recommendations on nuclear and other radioactive material out of regulatory control', *IAEA Nuclear Security Series No 15*, 2011, <https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control>
- [7.2] ANSI/IEEE N42.42 Standard, NIS, <https://www.nist.gov/programs-projects/ansieee-n4242-standard>
- [7.3] IEC 63047:2018 | IEC Webstore, <https://webstore.iec.ch/publication/28999>
- [7.4] Ec.europa.eu, ITRAP±10, <https://ec.europa.eu/jrc/sites/jrcsh/files/itrap10-summary-report-2016.pdf>
- [7.5] CORDIS, European Commission, SCINTILLA, <https://cordis.europa.eu/project/rcn/102073/factsheet/en>

- [7.6] C-BORD Project - Effective Container Inspection at BORDER Control Points -
Effective Container Inspection at BORDER Control Points,
<https://www.cbord-h2020.eu>

List of abbreviations

ARC	advanced reachback centre — national or international
BfS	Bundesamt für Strahlenschutz (Germany)
CAS	central alarm station
CBRN	chemical, biological, radiological and nuclear
CBRNE	chemical, biological, radiological, nuclear and explosive
CEA	Centre d'Etude Atomiques (France)
CNER	Centre National d'Expertise Radiologique (France)/National Centre for Radiological Expertise
CONOP	concept of operations
DU	depleted uranium
ERNICIP	European Reference Network for Critical Infrastructure Protection
eTTX	electronic tabletop exercise
FLO	front-line officer
GICNT	Global Initiative to Combat Nuclear Terrorism
GPS	geographical positioning system
HPGe	high-purity germanium
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IoT	internet of things
JRC	Joint Research Centre
LAT	latitude
LON	longitude
MEST	mobile expert support team
MORC	material out of regulatory control
MPE	major public event
NRC	national reachback centre
NSDA	nuclear security detection architecture
PPE	personal protective equipment
R&D	research and development
REPO	RElocatable POrtal monitor
RN	radiological and nuclear
PRD	personal radiation detector
RID	radioisotope identification device
RPM	radiation portal monitor
SOP	standard operating procedure
STUK	Radiation and Nuclear Safety Authority (Finland)

Appendix 1. List of items needed for the development of reachback capabilities

Reachback capabilities could be categorised into three levels ⁽¹⁾. This classification is notional and does not mean that a national expert support system must strictly belong to any of these groups. The development of reachback capabilities starts from the needs assessment in relation to handling potential RN events. All EU Member States should consider developing at least level-1 mechanisms and capabilities.

Level 1

Minimum requirements for the capabilities of expert support

- Legal basis of expert support exists — roles and responsibilities are defined at national level.
- Point of contact is declared at the national level.
- Mechanism for reliable and secure information sharing is developed.
- Mechanism to receive international assistance exists.
- Mechanism to support national threat and risk assessment exists.
- Capability to provide RN advice to responsible authorities 24/7 has been developed.

Level 2

Expert support centre is established

As above plus the following.

Technical support:

- implementation and maintenance of detection systems training and exercises
- safe and secure handling of radioactive sources
- participation in international exercises and comparisons.

Scientific support:

- assessment of alarms
- deployment of an expert team to support field mission.

Level 3

Advanced expert support centre is established

As above plus the following.

Operational support:

- role within national RN response framework 24/7
- role within national CBRNE response framework
- deployment of expertise at the crime scene
- rendering safe open sources.

Advanced technical and scientific support:

- advanced analysis support 24/7
- adjudication of alarms
- operation of large real-time detection systems
- capability to characterise radioactive material
- delivery of international assistance when requested
- execution of nuclear forensic investigations
- establishment of national nuclear forensics library

⁽¹⁾ The list of reachback capabilities is based on a lecture given by Harri Toivonen entitled '[Reachback: a crucial cross-cutting element of nuclear security detection architecture](https://erncip-project.jrc.ec.europa.eu/sites/default/files/ReachbackWorkshop-Toivonen-28Mar2017.pdf)' at Magic Maggiore — Technical Reachback Workshop, EC/JRC/ERNICIP and GICNT, ISPRA, 28-30 March 2017 (available at <https://erncip-project.jrc.ec.europa.eu/sites/default/files/ReachbackWorkshop-Toivonen-28Mar2017.pdf>).

- R&D on systems and measures
- modelling of nuclear and radiological detection systems and special detection geometries
- dispersion modelling (together with meteorological office).

Recommendation on basic capabilities for a reachback centre

The different studies presented in this document demonstrate that some capabilities have to be gathered for reachback centre operability, to reach the generic goal: reliable and remote RN support from a reachback centre for the units in the field. The operational aim of the reachback centre is to distinguish between 'false', 'innocent' and 'true' alarms, and moreover, if an alarm is 'true', to help define whether it is a radiological safety issue or a more threatening security issue.

The minimum needs, leading to basic capabilities, are of two types:

- material
- human.

Both of these can be separated into two groups:

- in the field
- in the reachback centre.

These groups are complementary: one cannot efficiently reach the goal without the other.

To set up basic capabilities, the recommendations are as follows:

- **Material, in-the-field:** radiation protection, source location and nuclide identification are the basic functions. To fulfil these functions, the team requires a contamination metre (alpha-beta probe), a gamma dose rate metre, a PRD or personal dosimeter, gamma detector for identification (RID or other spectrometer), a neutron counter and PPE.
- **Human, in-the-field:** any first responder with own skills, having completed specific RN training (on radiation protection, how to use the detectors, etc.).
- **Reachback, material:** a computing system with dedicated software for receiving, reading and analysing data (gamma spectra in particular).
- **Reachback, human:** a specialist in radiation protection and gamma spectrometry.

A complementary link between the field and the reachback centre is very important, to transfer information conveyed by both voice and data: phone, internet, satellite, etc.

All of the functionalities must be prepared jointly, together with the different stakeholders involved, and then tested, before ensuring their continual improvement through training and exercises. To reach the goal of basic capabilities, agreement on both sides (field and reachback), dedicated and designated people and, if possible, joint procedures and validated operating modes are necessary.

The first step in setting up a reachback centre is often the most difficult. To support this, especially if there is a lack of experts, a bilateral agreement could be made with another state or with an organisation, so that courses and training in the specific area of RN can be provided for personnel.

Appendix 2. List of publications of the ERNCIP RN Thematic Group, 2014-18

List-mode data acquisition

Peräjärvi, K., Keightley, J., Paepen, J., Tengblad, O. and Toivonen, H., *List-mode data acquisition based on digital electronics – State-of-the-art report*, Publications Office of the European Union, Luxembourg, 2014, <https://erncip-project.jrc.ec.europa.eu/documents/list-mode-data-acquisition-based-digital-electronics-state-art-report>

Paepen, J., Gårdestig, M., Reppenhagen Grim, P., Keightley, J., Nilsson, J., Peräjärvi, K., Tengblad, O. and Toivonen, H., *Critical parameters and performance tests for the evaluation of digital data acquisition hardware*, Publications Office of the European Union, Luxembourg, 2014, <https://erncip-project.jrc.ec.europa.eu/documents/critical-parameters-and-performance-tests-evaluation-digital-data-acquisition-hardware>

Paepen, J., Keightley, J., Peräjärvi, K., Tengblad, O., Grim, P. and Röning, J., *Standardisation of the data format for list-mode digital data acquisition: survey results*, European Atomic Energy Community, 2015, <https://erncip-project.jrc.ec.europa.eu/documents/standardisation-data-format-list-mode-digital-data-acquisition-survey-results>

Reachback

Toivonen, H., Reppenhagen Grim, P., Tengblad, O., Keightley, J., Paepen, J., Abbas, K., Schneider, F., Nilsson, J. and Peräjärvi, K., *Remote expert support of field teams – reachback services for nuclear security*, Publications Office of the European Union, Luxembourg, 2014, <https://erncip-project.jrc.ec.europa.eu/documents/remote-expert-support-field-teams-reachback-services-nuclear-security>

Toivonen, H., Schoech, H., Reppenhagen Grim, P., Pibida, L., James, M., Zhang, W. and Peräjärvi, K., *National reachback systems for nuclear security*, Publications Office of the European Union, Luxembourg, 2015, <https://erncip-project.jrc.ec.europa.eu/documents/national-reachback-systems-nuclear-security>

Toivonen, H., Reppenhagen Grim, P., Schoech, H., Keightley, J., Tengblad, O., Schneider, F., Forsberg, C. -J., Gattinesi, P. and Peräjärvi, K., *Information sharing in a nuclear security event*, Publications Office of the European Union, Luxembourg, 2015, <https://erncip-project.jrc.ec.europa.eu/documents/information-sharing-nuclear-security-event>

Tengblad, O., Peräjärvi, K., Toivonen, H. and Gattinesi, P., *After-action analysis of the Magic Maggiore Workshop on expert support and reachback*, Publications Office of the European Union, Luxembourg, 2017, <https://erncip-project.jrc.ec.europa.eu/documents/after-action-analysis-magic-maggiore-workshop-expert-support-and-reachback>

Robotics

Schneider, F. E., Gaspers, B., Peräjärvi, K. and Gärdestig, M., *Possible scenarios for radiation measurements and sampling using unmanned systems*, Publications Office of the European Union, Luxembourg, 2014, <https://erncip-project.jrc.ec.europa.eu/documents/possible-scenarios-radiation-measurements-and-sampling-using-unmanned-systems>

Schneider, F. E., Gaspers, B., Peräjärvi, K. and Gärdestig, M., *Current state of the art of unmanned systems with potential to be used for radiation measurements and sampling*, Publications Office of the European Union, Luxembourg, 2015, <https://erncip-project.jrc.ec.europa.eu/documents/current-state-art-unmanned-systems-potential-be-used-radiation-measurements-and-sampling>

Schneider, F. E. and Gaspers, B., *Survey on the use of robots/unmanned systems in scenarios involving radiological or nuclear threats*, Publications Office of the European Union, Luxembourg, 2015, <https://ec.europa.eu/jrc/en/publication/survey-use-robots-unmanned-systems-scenarios-involving-radiological-or-nuclear-threats-erncip>

Schneider, F. E., Gaspers, B., Keightley, J., Röning, J. and Paepen, J., *The unmanned systems trial for radiological and nuclear measuring and mapping*, Publications Office of the European Union, Luxembourg, 2017, <https://erncip-project.jrc.ec.europa.eu/documents/unmanned-systems-trial-radiological-and-nuclear-measuring-and-mapping>

Novel technologies

Ihantola, S., Tengblad, O., Toivonen, H., Peräjärvi, K., Csome, C., Borg, J., Paepen, J., Tagziria, H. and Gattinesi, P., *Novel detection technologies for nuclear security*, Publications Office of the European Union, Luxembourg, 2018, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC112304/jrc112304_novel_detection_technologies.pdf

Other publications

Toivonen, H., *Summary of the activities of the RN Thematic Group in 2016*, Publications Office of the European Union, Luxembourg, 2016, <https://erncip-project.jrc.ec.europa.eu/documents/summary-activities-rn-thematic-group-2016>

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: <http://europa.eu/contact>

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: <http://europa.eu/contact>

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: <http://europa.eu>

EU publications

You can download or order free and priced EU publications from EU Bookshop at: <http://bookshop.europa.eu>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see <http://europa.eu/contact>).

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub
ec.europa.eu/jrc



@EU_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub



Publications Office

doi:10.2760/365006
ISBN 978-92-79-98659-8