National reachback systems for nuclear security

State-of-play report

ERNCIP Thematic Group Radiological and Nuclear Threats to Critical Infrastructure
Task 3B Deliverable 1

Harri Toivonen, HT Nuclear Oy
Hubert Schoech, CEA
Per Reppenhagen Grim, DEMA
Leticia Pibida, NIST
Mark James, AWE
Weihua Zhang, HC
Kari Peräjärvi, STUK

2015

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.

EUR 27626 EN

Joint
Research
Centre

National reachback systems for nuclear security

JRC Science Hub
https://ec.europa.eu/jrc

JRC 98711

EUR 27626 EN

ISBN 978-92-79-54066-0

ISSN 1831-9424

doi:10.2788/718077

ERNCIP THEMATIC GROUP for Radiological and Nuclear Threats to Critical Infrastructure

National reachback systems for nuclear security

State-of-play report

November 2015

Kari Peräjärvi, STUK, Finland	Coordinator of the Task Group
Harri Toivonen, HT Nuclear Oy, Finland	Lead scientist of this report

Other main contributors to the report:

Hubert Schoech	CEA	France
Per Reppenhagen Grim	DEMA	Denmark
Mark James	AWE	United Kingdom
Leticia Pibida	NIST	United States
Weihua Zhang	HC	Canada

RN Thematic Group Members who also attended the reachback meetings:

Olof Tengblad	CSIC	Spain
John Keightley	NPL	UK
Jan Paepen	JRC-IRMM	EC
Jonas Nilsson	Lund University	Sweden
Magnus Gårdestig	Linköping University	Sweden
Frank Schneider	Fraunhofer FKIE Institute	Germany
Bastian Gaspers	Fraunhofer FKIE Institute	Germany
Jolien van Zetten	NEN	Netherlands
Carl-Johan Forsberg	ERNCIP Office	
Peter Gattinesi	ERNCIP Office	

Summary

Operational systems for nuclear security in Finland, France, Denmark, UK, US and Canada were reviewed. The Finnish case is a holistic approach to Nuclear Security Detection Architecture, as defined by the International Atomic Energy Agency; reachback is only one component of the system, albeit an important crosscutting element of the detection architecture. The French and US studies concentrate on the reachback itself. The Danish nuclear security system is information-driven, relying on the cooperation of the competent authorities. The British and Canadian analyses describe nuclear security planning and operations in a major public event (MPE), the Olympics, where cooperation between the frontline officers and the reachback centre plays a key role in reducing radiological and nuclear risks.

For the implementation of an efficient reachback system there is a strong need for standardising the data acquisition, storing and final distribution of the analysis results. Major nuclear powers take this activity very seriously, and they have 24/7, all-year national service for information processing. The case studies of Finland and France show that efficient European reachback is manageable and technically possible on a country-wide basis. The case study on Denmark reveals that countries with limited reachback resources need an adequate and standardised technical information-sharing mechanism to aid their national analysis services in a precise and timely manner.

Contents

Acronyms

AWE	Atomic Weapons Establishment, UK
CBRNE (CBRN-E)	chemical, biological, radiological, nuclear and explosive
CEA	*Commissariat à l'énergie atomique et aux énergies alternatives* — French atomic and alternative energies commission
CEN	*Comité Européen de Normalisation*; European Committee for Standardisation
CENELEC	*Comité Européen de Normalisation Électrotechnique*; European Committee for Electrotechnical Standardisation
CONOPS	concept of operations
CSIC	Spanish national research council
DCI	*Détachement Central Interministériel* — Inter-Ministerial Central Detachment, French police organisation (CEA is involved as a technical support)
DEMA	Danish Emergency Management Agency
DHS	Department of Homeland Security
ERNCIP	European Reference Network for Critical Infrastructure Protection
ERO	emergency response officer, US
FIFO	first in, first out; manipulate data buffer
FRAT	Federal Radiological Assessment Team, Canada
HC	Health Canada
IAEA	International Atomic Energy Agency
IND	improvised nuclear device
IRMM	Institute for Reference Materials and Measurements, belongs to JRC
JRC	Joint Research Centre, the European Commission's in-house science service
LINSSI	LINux System for Spectral Information, open-source database
LML	Linssi Markup Language (XML)
LOCOG	London Organising Committee for the Olympic Games
MORC	material out of regulatory control
NaI	sodium iodide, scintillator crystal used in gamma spectrometer
NEN	Netherland Standardisation Institute
NIST	National Institute of Standards and Technology, United States
NNSA	National Nuclear Security Administration
NORM	naturally occurring radioactive material
NPL	National Physical Laboratory, United Kingdom
NSDA	nuclear security detection architecture
ODA	Olympic Delivery Authority
POC	Park Operations Centre of London Olympics
PRD	personal radiation detector
PVT	polyvinyltoluene, plastic scintillator
RCMP	Royal Canadian Mounted Police
RDD	radiological dispersal device
RED	radiation exposure device
REPO	relocatable portals, Finnish national NSDA project
RID	radionuclide identification detector
RN	radioactive and nuclear materials
RPM	radiation portal monitor
SOH	state of health
SOP	standard operating procedure
SQL	structured query language
STUK	*Säteilyturvakeskus*, Radiation and Nuclear Safety Authority, Finland
XML	extensible markup language

1 Introduction

Successful interoperability of nuclear and radiological detection systems requires that European and international standards are devised for data formats and communication protocols. The European Standards organisations Comité Européen de Normalisation (CEN) and Comité Européen de Normalisation Électrotechnique (CENELEC) have accepted the Mandate M/487 to establish security standards for civil security applications (Final report of M/487 phase 2) ([1]); see also European Commission Action Plan for innovative and competitive security industry referring to, inter alia, risks on chemical, biological, radiological and nuclear material, including explosives (CBRN-E).

The European Reference Network for Critical Infrastructure Protection office (ERNCIP) ([2]) has established a thematic group on the protection of critical infrastructure from radiological and nuclear threats (RN thematic group) which looks at issues such as certification of radiation detectors, standardisation of deployment protocols, response procedures and communication to the public, e.g. in the event of criminal or unauthorised acts involving nuclear or other radioactive material out of regulatory control. The work is closely related to the opportunity, opened by the current developments in technology, of utilising remote support of field teams (reachback) for radiation detection.

The RN thematic group has worked with the following three issues:

1. List-mode data acquisition for radionuclide activity measurements based on digital electronics. The time-stamped list-mode data format produces significant added value when compared to the more conventional spectral data format. It improves source localisation and allows signal-to-noise optimisation and noise filtering, with some new gamma and neutron detectors actually requiring list-mode data to function. The list-mode approach also allows precise time synchronisation of multiple detectors enabling simultaneous singles and coincidence spectrometry such as ultraviolet-gated gamma spectrometry, among others.
2. Expert support of field teams, i.e. data moves instead of people and samples. Faster and more appropriate response can be achieved with fewer people. Optimal formats and protocols are needed for efficient communication between frontline officers and reachback centre.
3. Remote-controlled radiation measurements and sampling using unmanned vehicles. There are several measurement and sampling scenarios that are too risky for humans to carry out. Applications envisaged are: reactor and other RN accidents, dirty bombs before and after explosion, search for nuclear and other radioactive material out of regulatory control.

This report describes the reachback approach in Finland, France, Denmark, UK, US and Canada (item 2).

([1]) http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/default.aspx

([2]) In support of EU efforts to protect critical infrastructures, the Joint Research Centre (JRC) coordinates ERNCIP, which was first established by the Institute for the Protection and Security of the Citizen in 2009. This took place under the mandate of DG HOME, in the context of the European Programme for Critical Infrastructure Protection. ERNCIP's mission is to 'foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities'.

2 Technical Reachback in Finland

Harri Toivonen, HT Nuclear Oy and Kari Peräjärvi, STUK

The Finnish competent authorities approach nuclear security in a comprehensive manner, information sharing playing the key role. Finland has integrated application-specific technologies and operations for close cooperation between the authorities [FIN, 2014]. This architecture includes mobile detection capabilities and portal monitors utilising reachback services. Raising awareness on nuclear security, training, and exercises ensures sustainability, and relocatable assets enable an adaptable architecture.

2.1 Finnish Nuclear Security Detection Architecture

The Finnish Nuclear Security Detection Architecture (NSDA), dealing with threats related to nuclear (N) and radioactive materials (R), is integrated with other threats from biological (B) and chemical (C) materials, and from explosives (E). Under the leadership of law enforcement agencies, special CBRNE teams are formed containing expertise from different competent authorities. CBRNE teams are prepared to search for nuclear and other radioactive material out of regulatory control (MORC) and respond to possible threats together with other national response organisations. CBRNE teams are deployed typically in operations before and during an MPE (sporting event, summit, etc.). The Radiation and Nuclear Safety Authority, STUK, provides real-time reachback services for these teams.

Technical requirements

The Finnish NSDA for the detection of MORC is built upon the existing national infrastructure and organisational structures. Special emphasis was placed on the fast resolving of alarms generated by the detection instruments. The systems and measures must be user friendly, sustainable and cost-efficient, and provide information which is useful for prompt countermeasures (wisdom). The following technical characteristics are required:

- mobile or relocatable spectrometers;
- data in the same format (XML);
- information transfer to a local database and to a central database in real time;
- expert analysis for interpretation of the findings.

Use of spectrometers

A key design basis of the NSDA is the low false alarm rate (< 10^{-6} per measurement) ([3]). This requirement is intended to eliminate the large burden of initial assessments of alarms. Therefore the instruments must exhibit radionuclide identification capabilities. New detectors in the NSDA are mainly based on low- and medium-resolution spectrometers, with large sodium-iodide (NaI) detectors acting as the workhorse in national border portal monitoring. Lanthanum-bromide, $LaBr_3$ spectrometers are used in backpacks; they have a better energy resolution than NaI detectors, and thus are better

([3]) International standards and false alarm requirements:
IEC 62401 (PRD). 'The number of false alarms shall be no greater than 1 alarm in 1 h.'
IEC 62244 (RPM). None in 100 h.
ANSI N42.38 (SRPM). 'When tested in an area with a stable background (only natural fluctuations) at the levels stated in Table 4, the false alarm rate shall be less than 1 per 1000 occupancies for systems that use occupancy sensors or one alarm over a 2 h time period for monitors that do not use occupancy sensors. In addition, the monitor shall not identify a radionuclide that is not present during the test period.' (Table 4 of the standard says that background exposure rate is less than 0.25 μSv/hr).

suited to mobile applications (with changing backgrounds) and can better resolve background peaks from

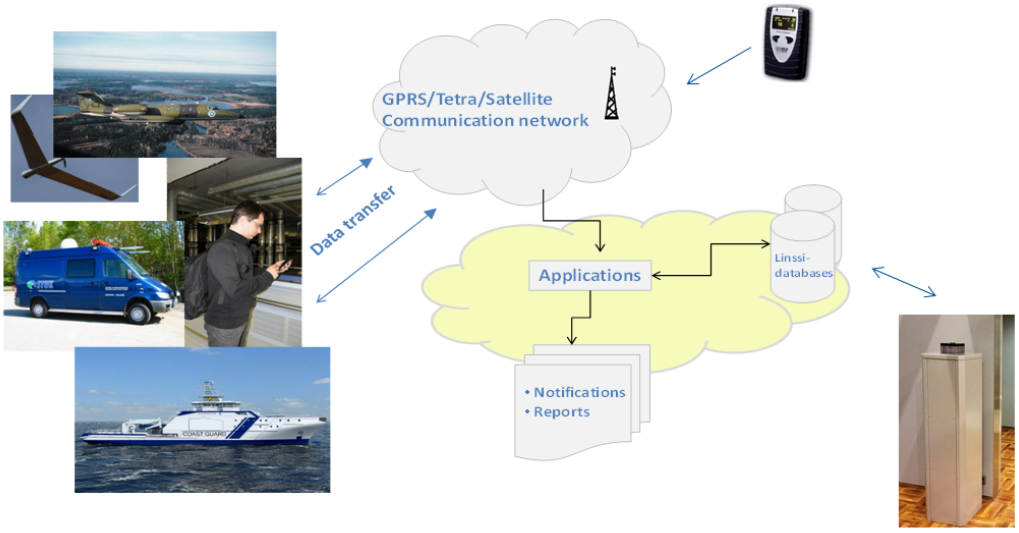

Figure 2.1. Mobile measurements connected to reachback centre. The spectra are transferred via wireless networks to a remote server (LINSSI). A subject matter expert analyses the findings using automated and interactive software, and gives advice to the frontline officers via secure voice communication. The architecture contains also portal monitors (see Figure 2.2).

peaks of interest (Figure 2.1). High-resolution spectrometry (HPGe detectors) is used by STUK in cases that cannot be resolved with other instruments.

Analysis of threat situations

Finnish authorities aim at building scenarios in a systematic manner to understand the true nature of the threat and risk. The aim is to identify gaps and to undertake corrective actions and design response resources in a balanced manner. Risk is the combined effect of a threat and its consequences [IAE, 2014].

National coordination for steering the cooperation between authorities

Nuclear security activities that concern MORC need to be nationally coordinated so that all activities are in agreement with national legislation, regulations and other provisions. A CBRNE Advisory Committee was formed within the Ministry of the Interior in 2015.

Information sharing as a cornerstone of authority activities

Efficient distribution and utilisation of correct information enables the optimisation of authority activities. Many kinds of operations and information users are connected to the NSDA (analyst, chief of operations, frontline officer, map specialist, IT personnel, spokesman). Getting correct information to the relevant users in a timely fashion is of paramount importance for the success of nuclear security tasks. Various technical and non-technical systems have been implemented, or planned, to improve information sharing.

Relocatable detection systems

The infrastructure in border crossing points, harbours in particular, is extremely complex, and essential changes are often made. Maintaining fixed portal monitors in these

conditions is a challenge, requiring new installation designs. On the other hand, often there is a short-term need for screening, either in special operations of customs or law enforcement, or other security authorities. Therefore, there is a need for detection systems that can be deployed rapidly, while retaining good performance capabilities. The new NSDA addresses sustainability and detection efficiency through relocatable ([4]) detection systems [IAE, 2011]. The instruments must have a wireless capability to transfer their data to a database in a local server, or even to a remote server.

Implementation of reachback

Technical information sharing between competent authorities is challenging. Often subject matter experts are not available at local level for the interpretation of the acquired data. In the new NSDA the interpretation of the key findings is performed remotely by an analyst located outside the site of action. The analyst is able to talk to the field officer during the operation using secure government communication network (Virve) which is based on Tetra standard ([5]).

Alarm adjudication requires automated, fast and reliable data transfer from the spectrometers to the databases of the competent authorities. For this purpose a comprehensive data management system was designed (see section 2.5).

Sustainability of human resources

Human resources within the NSDA need to be sustained. This is a major issue for a small country with a small pool of experts. The competent authorities arrange awareness and training courses and exercises, where all key organisations are involved. Every year there are security-related events that give the response organisations a possibility to test their interoperability in practice.

Research and development for national needs

National research and development programmes are necessary to provide detection technology that suits the existing security infrastructure and concept of operations (CONOPS). For example, the research carried out in STUK led to the conclusion that NaI(Tl) gamma spectrometers are also very sensitive neutron detectors if they are operated over a wide energy range [HOL, 2012]. This cost-effective approach is already implemented in the detection systems at the Helsinki airport and other border crossing points. Without compromising neutron detection capability, the new approach provides immediate cost savings in investments of the order of several million euros. Furthermore, the integrated detection system is technically simple to operate as compared to two separate systems consisting of photon and neutron detectors. This is a great advantage for the sustainability of the entire NSDA.

([4]) These are sometimes called portable radiation scanners (e.g. backpacks), and mobile and transportable radiation monitors. Mobile systems operate during the move, transportable operate at the point of installation, but not during the move.

([5]) Tetra telecommunication standard (http://www.tandcca.com/about/page/12320).

2.2 Technology Development for Nuclear Security Detection Architecture

The management of threats forms the basis of the architecture design which addresses legal, organisational, operational, regulatory and technical aspects of nuclear security. A new model for the authority cooperation was created, countering criminal and terrorist activities.

With a comprehensive architecture, response can be made cost-effective. This requires that the technology is interoperable and data transfer happens in real time, regardless of where activities are taking place. An essential part of the technology is the analysis of acquired data and sharing of information between experts and operative personnel. Defining the needs and performance requirements of the authorities is an important part of the detection architecture.

The development of authority cooperation in Finland started from practical needs. Field activities and information processing related to nuclear and other radioactive materials have been developed by strongly committed experts of the Helsinki Police Department, Helsinki City Rescue Department, Customs, Finnish Defence Forces and STUK.

The NSDA was developed in a project called REPO. The acronym refers to 'Relocatable Portal' monitoring. However, REPO covers technical systems and measures that reach far beyond border monitoring, including the interior and exterior layer of the detection architecture. The first phase of the project (2012-2013) focused on developing a conceptual framework for the management of threats concerning MORC. The authorities collaboratively defined the detection technology that will be used, at least to the proof-of-concept level. The key requirement was that the detection instruments must be able to transfer their findings in real time to the database used by the authorities. In the second phase (2014-2016) the companies are given an opportunity to demonstrate their solutions. The implementation of the REPO project concentrates on technical solutions based on interplay between frontline officers and the technical reachback centre [FIN, 2014].

2.3 Operations Centre and Reachback

A key crosscutting element of the NSDA is the Operations Centre, which is responsible for maintaining situational awareness of radiological and nuclear detection capabilities and for facilitating the coordination of responses. The operations centre has access to all information on threat and capabilities to interdict. In nuclear security, the law enforcement authority has the leadership. For cooperation between STUK and law enforcement a technical reachback mechanism was established to engage scientists and analysts in assisting with technical expertise for investigating and resolving alarms. Reachback assists frontline officers at the site of action for the adjudication of alarms.

2.4 Field operations

The technical layer of the NSDA has to deal with fixed portals and mobile measurement systems. The fixed portals are large sensitive devices to monitor daily traffic at border crossing points and other critical sites. The mobile systems provide unpredictability; the adversaries cannot know the capability of the authorities. Both of these detection systems act as a deterrent.

Fixed portal monitors

The Finnish Customs have systematically built radionuclide detection capabilities. Sensitive spectral devices are installed at the borders and other strategic locations. The measurement system, containing several detection instruments, cameras and alarm-handling software, produces a massive amount of data every day. The data acquisition interval of NaI-spectrometers used by the Finnish Customs is 1 or 2 s. At a border crossing point there may be 10 or more instruments. Therefore, its daily volume may approach one million spectra, and these need to be analysed locally and remotely by radionuclide experts. In addition, procedures must be in place for alarm clarification processes performed by the customs officers, together with the reachback centre.

Mobile search

Mobile search capability is a cost-efficient way of increasing detection and response capacity. However, such a system creates a large amount of complex data, including background radiation which changes continuously. The non-constant background radiation creates an inherent problem of false initial alarms. For correct response the spectra must be assessed in a timely manner by an analyst with experience in nuclear spectrometry. Such a response is difficult or impossible to realise on the site, as there are not sufficient human resources (experts) for this task. Automated data transfer and reliable data processing provide the solution. This was the initial basis of the establishment of a technical reachback centre in STUK.

In the new concept the expert is no longer deployed to the field. Thus, the non-expert field teams need to be trained in basic radiation protection, radiation measurement equipment and search techniques. The expert analysing the information in the reachback organisation must have enough quality assurance data to verify that the measurements are correctly performed. The Finnish reachback uses automated analysis processes in the initial phase of alarm adjudication but the final say (knowledge) comes from an expert through an interactive process.

2.5 Data Management and Reachback Software

The reachback capability was initially implemented through software, known as *SNITCH*, Spectral Nuclide Identification Technology for Counterterrorist and Hazmat units. Later, the software was split into two parts: *SNITCH* and *REACHBACK*, the former takes over data management, including control of input operations to a database through a FIFO process (first in, first out), whereas the latter is a reporting package based on Java and web tools taking their input from the database. The FIFO tasks are processed in the order that the system received the tasks. Currently, four data exchange (upload) interfaces have been implemented: email message, web browser, web services and cloud services. The data acquisition software can also write directly to the database.

The data server (DS) and the analysis server (AS) contain a software package that automates the handling of spectrometric measurement and analysis information (Figure 2.2). The data server automatically inserts the received information onto the database and launches several processes depending on the type and properties of the uploaded information. Any type of processes can be created for the analysis server, but typically they are notifications and automated analyses. Notification processes inform the users or experts that new information has been uploaded, or they send short operational text messages (< 140 characters) to frontline officer, duty officer or experts. Analysis

processes are launched to analyse automatically the new information. The users are of two different

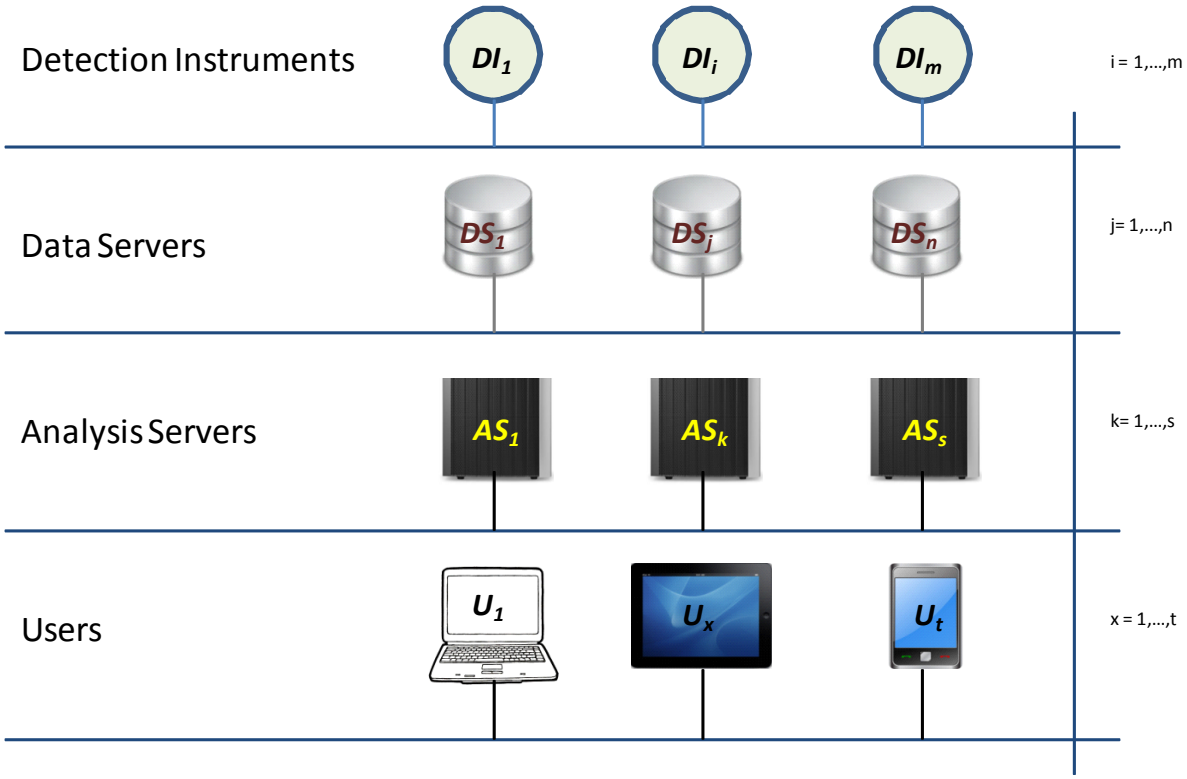

Figure 2.2. Data acquisition, analysis and management in Finnish Nuclear Security Detection Architecture. Any detection instrument (DI) can write its data to any data server (DS); one or more analysis servers (AS) can be configured to analyse data in any server, including automated and interactive processes. The end users (U) have access to the data and analysis results via web browser or dedicated tools, such as analysis and reporting software. Each data server runs a FIFO process. The master process keeps track of what needs to be done next. The slave processes, which can be anywhere in the network, perform the tasks and inform the master when the process is finished. The slaves work in parallel, and the capacity can be made as large as needed for a timely output. The slaves report their findings to the very same database where they got the task from the master.

types: (i) radionuclide experts who can view and examine the data interactively, giving priority to the most important findings and alarms; (ii) users, who can also be a frontline officer or be located at the operations centre and receive knowledge useful for the clarification process to produce wisdom for the response.

The data management software provides a user-friendly way to exchange measurement data and analysis results. The data exchange is fully automated in short intervals (typically 1-4 s) and no user actions are needed. However, the data can also be sent to the system manually. This is useful for inspection of suspicious targets at border crossings or customs, for example.

References

[FIN, 2014] Finnish nuclear security detection architecture for nuclear and other radioactive material out of regulatory control. REPO — Nuclear security development project. Final report of phase one. Public version, 2014. http://www.stuk.fi/repo-eng.

[HOL, 2012] Holm P., Peräjärvi K., Sihvonen A.-P., Siiskonen T., Toivonen H.. Neutron detection with a NaI spectrometer using high-energy photons. Nuclear Instruments and Methods in Physics Research A 2013; 697: 59–63. DOI:10.1016/j.nima.2012.09.010 **(**Epub 2012 Sep 12.**)**

[HOL, 2014] Holm P., Peräjärvi K., Sihvonen A.-P., Siiskonen T., Toivonen H.; A capture-gated neutron spectrometer for characterisation of neutron sources and their shields; Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment; Volume 751, 1 July 2014, Pages 48–54; DOI: 10.1016/j.nima.2014.03.021.

[IAE, 2011] International Atomic Energy Agency. Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control. IAEA NSS-15, Nuclear Security Series 15, Vienna 2011.

[IAE, 2012] International Atomic Energy Agency. Nuclear Security Systems and Measures for Major Public Events. IAEA NSS-18, Nuclear Security Series 18, Vienna 2012.

[IAE, 2013] International Atomic Energy Agency. IAEA. Nuclear Security Systems and Measures for the Detection of Nuclear and other Radioactive Material out of Regulatory Control. IAEA NSS-21, Nuclear Security Series 21,Vienna 2013.

[IAE, 2104] International Atomic Energy Agency. Threat Assessment and Risk-Informed Approach for Implementation of Nuclear Security Measures for Nuclear and other Radioactive Material Out of Regulatory Control, IAEA Nuclear Security Series (Draft), Vienna, 2014.

3 French Reachback Approach and Management

Hubert Schoech, CEA

The French Atomic and Alternative Energies Commission, CEA, is mandated by authorities in different CBRN-E actions. Especially for the RN threats, CEA has a mandate to support any first responder and state forces, as part of the 'DCI' missions (French police organisation where CEA is involved as a technical support). One of these tasks is the collection and subsequent analysis of RN data, in order to assess a threat and give a quick answer and advice to the first responders. The experts performing analyses are located away from the field, at a CEA facility, where they are able to process the data remotely. This off-the-scene capability forms the French Reachback Desk, called 'Triage', which is on duty 24/7.

If a threat is confirmed, the French response capability is activated and led by DCI.

3.1 Reachback Definition

What is called 'reachback' in some countries is called 'triage' in France. The word 'reachback' is reserved for classified activities conducted in relation with the French response to RN threats, while 'triage' is used in the context of initial threat assessment, i.e. whether it is a RN threat or not (threatening device or a health and safety issue).

The classified capabilities that are part of the French reachback will not be discussed in this paper. Collaboration with other countries concerning the 'triage' mode is open and welcome.

For a better understanding and consistency with the other parts of the document, either the general term reachback or the term triage are used, both in the same sense.

3.2 Triage/Reachback Main Capabilities

The French triage/reachback capacity has a national coverage, and is operational since mid-2012. Currently, the triage missions for the CEA experts mainly consist of analysing gamma spectra and giving advice on radiological protection issues (health and safety), as well as collecting and analysing complementary incoming information (pictures, dimensions, other RN data, etc.).

Two concurrent analyses are performed and checked by two CEA experts, which are on duty 24/7. In closed hours, the data are available through an everywhere-connected laptop.

The analyses have to be performed as quickly as possible, with some warning parameters (head office immediately informed), and the final results are sent to the RN head officer less than 30 minutes after data receipt. Coupled to information received from other components of the DCI office, a decision is taken about the threat level, with the aim of sorting out between a real RN threat and a radiological problem. Avoiding activating the full French response capacity on a false alert is almost as important as detecting a real threat.

If needed, the Triage Desk may request additional measurements from the first responders, while the first responders may ask for radiological advice or details about the handheld detectors/spectrometers.

Concerning the analysis of gamma spectra, both commercial-adapted and internal CEA software and algorithms are currently used, always with the intent of checking manually the automated analysis. Currently, most of the data are sent to the Triage Desk by email. Since the CEA experts are not continually in front of the computer screen, the first responders have first to contact the Triage Desk by phone in order to inform that they are ready to send data. International receipt is possible, after the petitioner has been allowed by the CEA to transmit data.

The triage/reachback infrastructure and capacity serves as a backbone for RN detection architectures. Such architectures have been tested in France. A pilot deployment project conducted and funded by the French inter-ministerial SGDSN (Secrétariat Général de la Défense et de la Securité Nationale) is currently implemented by CEA in several critical infrastructures. Also, CEA is part of RN detection architecture deployment projects in foreign countries, especially in the context of EU CBRN Centres of Excellence (Project #24).

3.3 Capabilities Linked to Triage/Reachback

CEA has expertise, knowledge and experience in several other domains, complementary to the triage/reachback capability itself. These other domains include:

Equipment testing:

- Dosimeter/Detector/Spectrometer capabilities are assessed in order to control performances announced in vendor datasheets and to get better knowledge about the limits of the equipment.
- A new 'RN metrology platform' has been built for accurate measurements (see Figure 3.1). It is composed of a linear 3-axes movable support, itself movable in a circular room, completed with a set of standard calibration sources and in the near future with an irradiator.
- According to each specific first responder's mission, CEA can help them to select the equipment best fit to their specifications, thanks to the study of several handheld detectors.

Training:

- Internal CEA specific training is performed, including software and hardware tools.
- 'External' training can be provided to first responders, starting with radiological protection and source search, up to first-level analysis and reachback data sending (training with real sources). Included in the 'RN metrology platform' and its vicinity, several rooms are available for both the theoretical and practical training courses.
- Adapted procedures and user's manual are published.

Connected devices:

- To transmit data from the field to the Triage Desk, the connectivity capability of the measurement systems is mandatory. Since this function is either non-existent or incomplete, CEA develops such a capability for an increasing number of systems.

All these facilities and services are available for any first responder or other allowed units, in order to achieve the most effective chain of measurement, from the first responder in the field up to the final data analysis results.

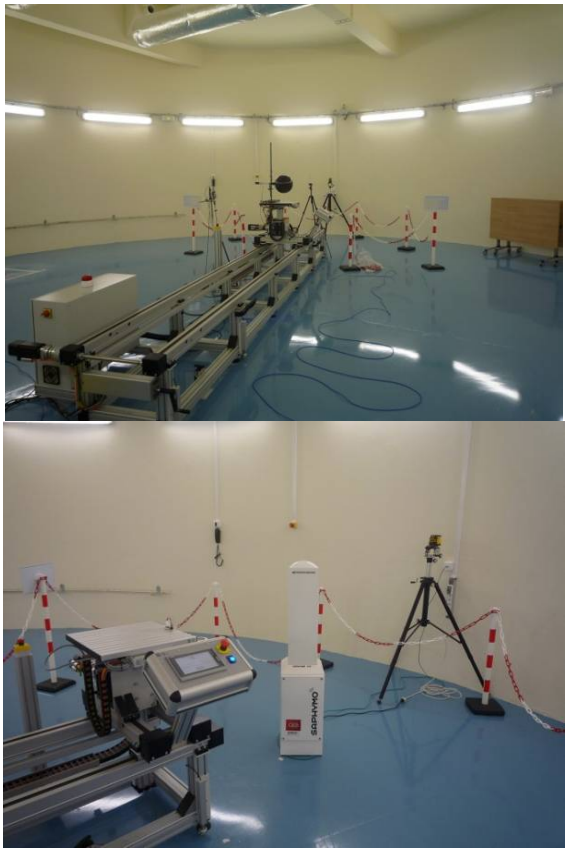

Figure 3.1. French RN metrology platform.

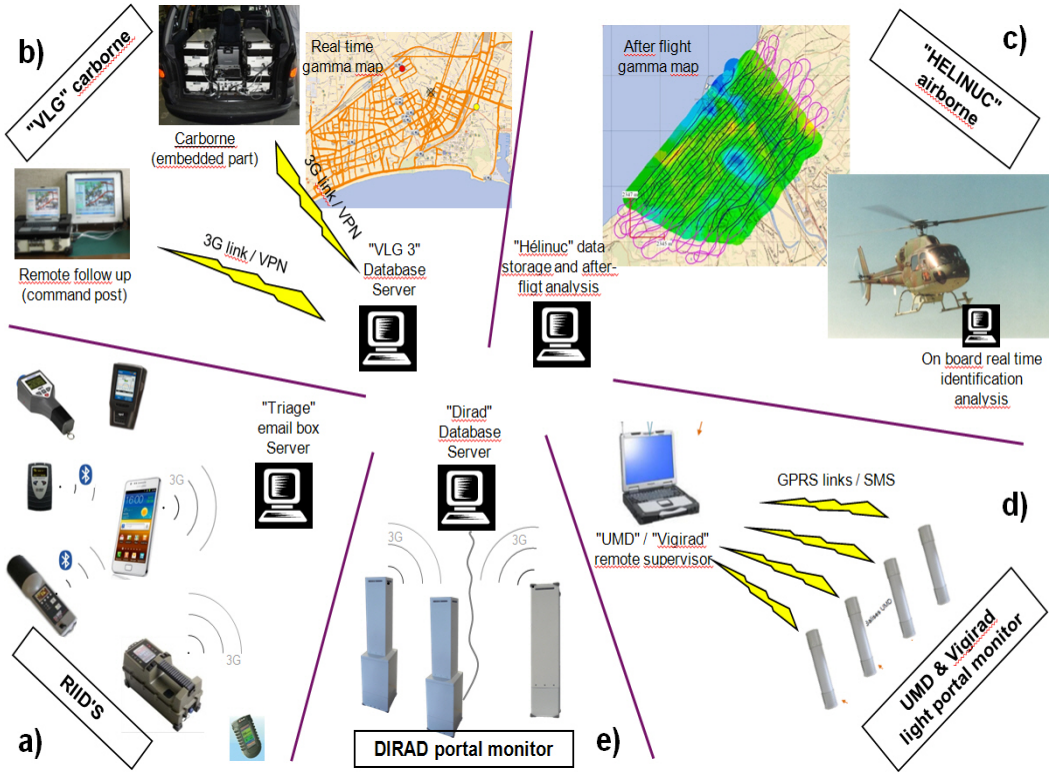

Figure 3.2. Some of French spectrometry systems currently deployed, most of them with different data transmission capabilities: a) handheld spectrometers, to triage email box, b) carborne system, to specific server, c) airborne gamma mapping, d) light portal monitors and e) heavy portal monitors, to specific servers.

3.4 Current means

Currently, as shown in Figure 3.2, several means (embedded, fixed or portable spectrometry systems) are deployed and operated by CEA response teams, first responders and other state forces. From pedestrian detectors up to aerial gamma mapping, different transmission solutions are operational or under development. Some of them are already operational for many years, including real time and non-stop data transmission systems (for example, the CEA carborne systems, called VLG).

3.5 Reachback in future

Feedback and experience is capitalised in the French centralised database, which implements a network connecting the detectors to a 'National RN Expertise Centre' (see Figure 3.3). This database was successfully tested and works now with several spectrometers (Spir-ID handheld spectrometer, DIRAD portal monitor, etc.) before becoming operational late 2015. This database is designed to be easily adaptable to any spectrometer in order to receive and archive data and other information (such as state-of-health, barrier's state, picture, etc.), whether the instrument is linked by wire or by other means. The database is designed to accept any existing and future commercial or internally developed equipment, with a simple 'plug and play' logic. It is an extensive, adaptable and high-capacity database, compatible with the LINSSI format.

Future upgrades are expected, for example to send data back to a laptop which can be located anywhere, in order to supervise the deployed systems even from the advanced headquarters (see Figure 3.3). This functionality is already available for many years for some of the internally developed systems (VLG3 carborne system, UMD & Vigirad light portal monitor systems) and would be generalised.

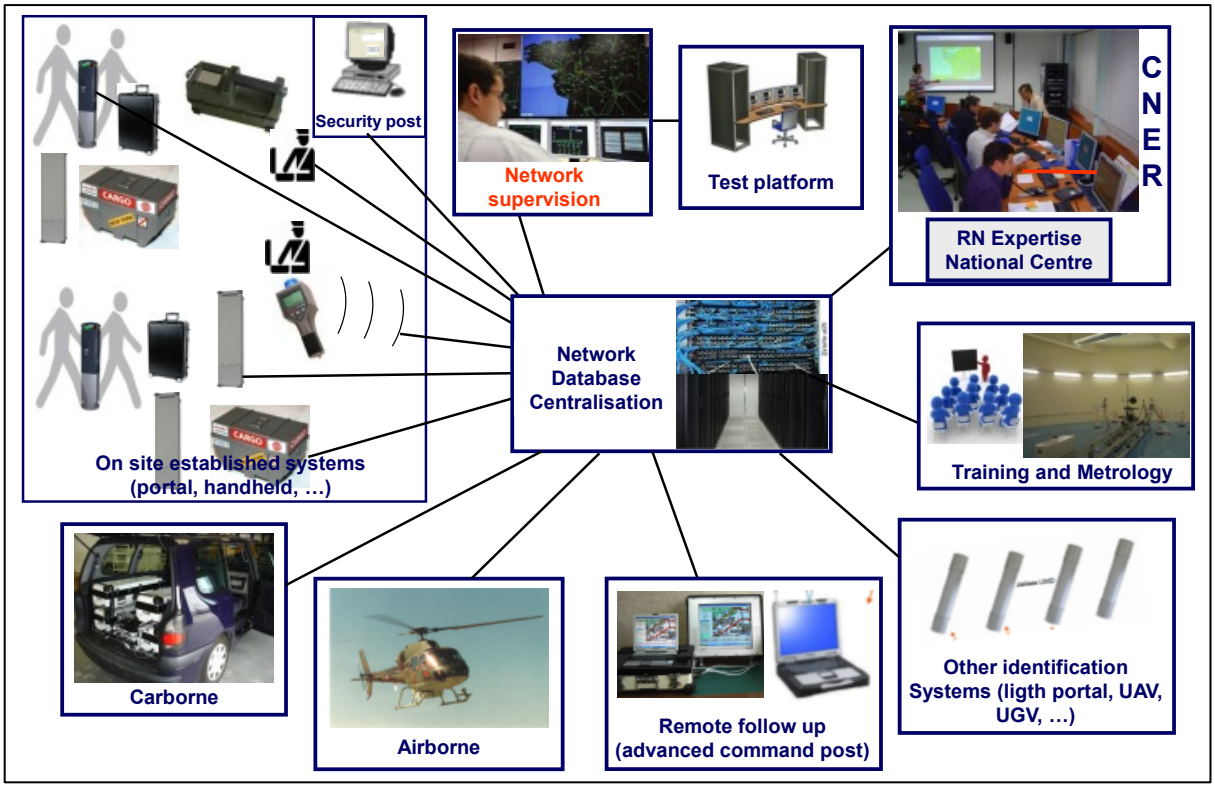

Figure 3.3. Future architecture of the French centralised network accepting input from any equipment.

4 Danish Reachback Approach

Per Reppenhagen Grim, DEMA

In Denmark the common approach to all major incidents is coordinated by the police, and technical issues are solved by other competent authorities. The leading role in a confirmed radiological or nuclear threat operation is conducted by the Danish Radiation Protection Agency and supported by the Nuclear Division of the Danish Emergency Management Agency. Another key player is the Danish Customs Administration. This setup includes mobile detection capabilities and portal monitors.

4.1 Danish Nuclear Security Direct Response

The Danish CBRNE security, dealing with threats related to nuclear and radioactive materials, is integrated with other threats from biological and chemical materials, and from explosives. Under the coordination of law enforcement, special CBRNE teams are formed with expertise from different competent authorities. CBRNE teams are prepared to search for nuclear and other radioactive material and respond to possible threats together with other local and national response organisations. CBRNE teams are deployed typically in operations before and during major events based on a thorough security evaluation. The reachback services for the RN part consist of laboratory (sample analysis) capacities and direct contact to the appropriate duty officer (on call 24 hours a day, all year).

4.2 Threat Detection

Direct and indirect threat detection plays a key role in Danish hazardous materials handling. Information sharing with national and international competent authorities is vital to the detection of possible threats and rapid and efficient response is the main factor in emergency management.

4.3 Reachback Main Capabilities

The Danish reachback capacity has a national coverage. The reachback tasks for the Danish experts mainly consist of analysing gamma spectra and giving advice on radiological protection issues (health and safety), as well as collecting and analysing complementary incoming information (pictures, dimensions, other RN data, etc.).

4.4 Future Needs Assessment

Denmark, with limited reachback resources, requires adequate, standardised and updated database tools to aid the national analysis capacities and to provide reachback services in a precise and timely manner.

5 Radiological Triage in the United States

Leticia Pibida, NIST

The radiological reachback or triage program in the US is operated by the National Nuclear Security Administration (NNSA) ([6]), and is part of the Global Nuclear Detection Architecture coordinated by the Department of Homeland Security (DHS). In addition to frontline officers, several different organisations can use reachback or triage. These organisations include the Radiological Assistance Program, the Search Response Team and the Nuclear Radiological Advisory Team.

5.1 Triage Goals and Implementation

The goals of the radiological reachback or triage is to provide a secured, online capability that provides remote support to frontline officers and emergency responders in the event of a nuclear or radiological emergency. It is also meant to provide essential time-sensitive information on the nature of the radiological incident; it is designed to provide information to the frontline officers within 30 to 60 minutes from receipt of the data. This information allows first responders to develop and implement appropriate courses of action without placing unnecessary demands on critical resources.

Triage expertise

The system is comprised of scientists and engineers from the NNSA's and the Department of Energy's (DOE) national laboratories. Scientists are available 24 hours a day all year to analyse site-specific data and confirm radionuclide identification in the event of a radiological incident. This requires knowledge on gamma-ray spectrometry and different types of radiation detection and identification systems used in the field. The scientists are on duty for one week every six weeks.

Steps in the triage response

Frontline officers resolve hundreds of alarms each day. They refer an alarm for resolution to reachback or triage according to:

- fixed rules (neutrons, plutonium indicated, etc.) or;
- experience and police intuition.

For border crossing events, data are referred to regional analysts with experience with many common events ([7]).

When an incident occurs, the frontline officer calls the NNSA 24-hour watch office to report the incident. The on-duty emergency response officer (ERO) takes the call and evaluates the situation. Some events are resolved by the ERO without the need of contacting a scientist. Depending on the situation, the ERO activates triage by contacting the scientist on call. The data collected by the frontline officer gets transmitted to an NNSA website. The data is sent to two scientists, each from a different laboratory (Los Alamos National laboratory, Lawrence Livermore National Laboratory, Sandia National Laboratory). The data analysis starts within 10 minutes from the time the ERO contacts the scientists. The data is analysed and the results need to be back within 30 to 60 minutes from the time the data was received. The ERO makes the final determination, not the scientists, since the data sent for analysis to the scientists is only a small part of

([6]) NNSA website: http://nnsa.energy.gov/
([7]) Material provided by George P. Lasche, at the 2010 IAEA meeting.

the information available associated with the incident at hand. For the alarms that still cannot be resolved, senior scientists attempt to resolve the alarm on an open telephone conference call convened by the ERO. In serious situations the Emergency Response Team is activated. Figure 5.1 shows a diagram of the triage process.

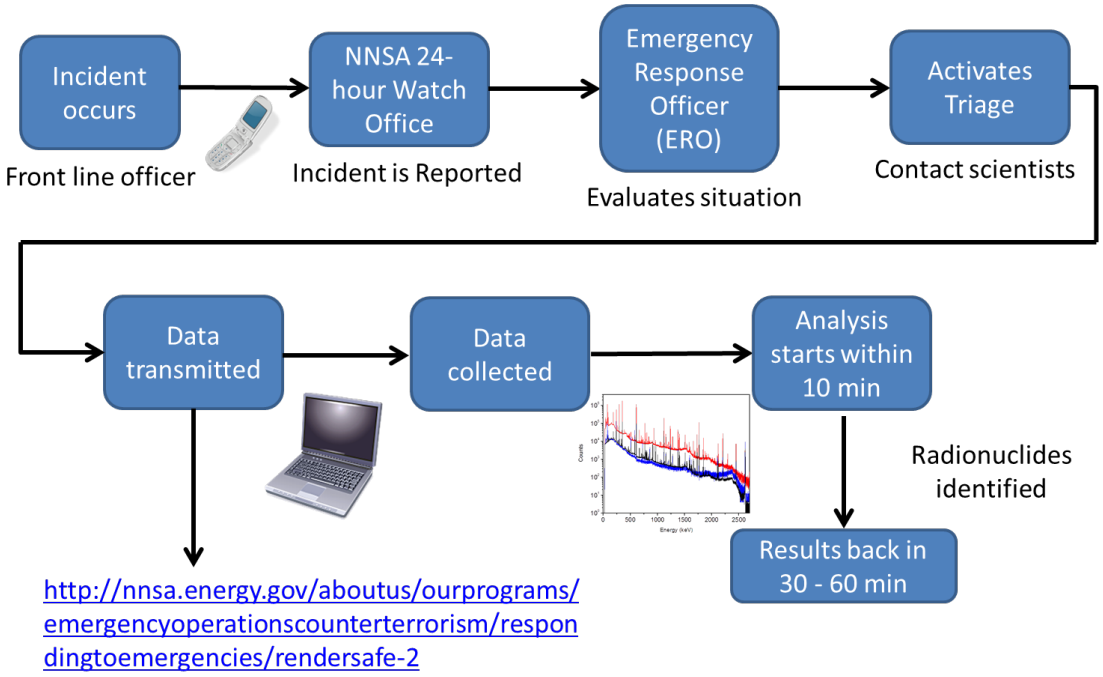

Figure 5.1. Reachback or triage process in the US.

5.2 Data Required for Analysis

The data transmitted by the frontline officer to the ERO may include:

- description of the circumstances;
- photos;
- measurements from radiation detection systems.

In order for the scientists to make a determination of the radiation item being analysed based on the measurements performed by the frontline officer they need to have the following information:

- full gamma-ray spectrum of the item;
- full gamma-ray background spectrum;
- neutron count rate if present.

In order to obtain the best possible results it is required to characterise the detection systems regarding:

- information about the radiation detection system response both for gamma-rays and neutrons;
- energy and efficiency calibration of the radiation detectors that are part of the radiation detection system;
- spectrum of a reference or check source at site (e.g. ^{232}Th).

Information regarding the radiation detection system response for gamma-rays and neutrons may be obtained by different means prior to an event. A library has been built in

order to catalogue the radiation detection system response of the different instruments deployed in the field.

Another critical component is the data format. Each manufacturer has its own proprietary software in order to analyse and display its instrument data. In addition, manufacturers sometimes make software updates to a given instrument model and the data structure gets modified, and such information might not be available to the instrument users. This creates an additional burden to the scientists as they first need to determine how to read the data before they can start the analysis. These issues lead to the development of the standards ANSI/IEEE N42.42 [ANS, 2006] and IEC 62755 [IEC, 2012].

References

[ANS, 2006] ANSI/IEEE N42.42. Data Format for Radiation Detectors used for Homeland Security, 2006.

[IEC, 2012] IEC 62755. Radiation Protection Instrumentation — Data Format for Radiation Instruments Used in the Detection of Illicit Trafficking of Radioactive Materials, 2012.

6 Radiation Screening at the London 2012 Olympics

Mark James, AWE

The London 2012 XXX Olympiad was a globally significant event, watched by billions and scrutinised like no other event before. With over 2.6 million spectators expected at the Olympic Park in Stratford, East London, the site was designated a 'Tier 1' security venue, meaning that the risk and consequences of a terrorist-related event would be both 'high' and 'catastrophic'. As a result, securing the Olympic Park against all conceivable threats was of the highest priority to the Cabinet Office in Whitehall and the Home Office, who oversaw all security arrangements. While no specific chemical, biological, radiological or nuclear (CBRN) threats had been made, the government recognised that a large-scale biological or radiological attack against the UK was amongst the highest impact risk scenario.

An ambitious multi-million-pound programme of work was undertaken which started in late 2010. In early 2011 a team from the Atomic Weapons Establishment (AWE) was invited to meet with the London Organising Committee for the Olympic Games (LOCOG), the Olympic Delivery Authority (ODA) and the Home Office in order to provide the programme with radiological detection expertise and advice. The Olympic Park was pre-screened for radioactive material during construction. Prior to the start of the Olympic Games the role of AWE was to provide technical guidance, threat assessment and assurance that the detection capability provided was able to meet the requirements that LOCOG/ODA and the Home Office had set. Additionally AWE was to support LOCOG during the games to investigate and resolve all radiation alarms at any of the entry points.

6.1 Challenge

One of the principal challenges was to develop a system that was both capable of detecting and identifying radiological material yet would not slow down the flow rate of people or vehicles entering the Olympic Park. It was recognised that park security personnel had no knowledge of radiation detection or the use of radiation detection equipment, and that training them would be both costly and time consuming. A system would therefore need to be developed that would minimise the interaction of the security personnel. By late 2011 such a system had been developed that would use a variety of commercial off-the-shelf radiation detection equipment fully integrated into one complete system. The final system was a multi-layered radiation screening system comprising large sodium iodide crystals with integrated identification algorithms, along with large-area plastic scintillation-based technologies to provide both low gamma count rate detection as well as localisation capability. These were augmented with a range of handheld radiation detectors for more discreet searching.

6.2 Preparation

During the construction of the Olympic Park two aerial surveys were carried out, the first several weeks before the events and the second just prior to 'lockdown'. The survey prior to lockdown was also supplemented with a ground survey. The data was then analysed at two UK establishments. The results of these surveys showed that there were no areas of concern and all measurements showed a typical background profile.

Estimates were made of the likely alarm rates expected in order to make the response suitable and sufficient for the event. For the pedestrian environment data was obtained

from a trial carried out by Mirion at Vienna Airport and from data provided by UK Border Force relating to pedestrian traffic at Heathrow Airport. The final estimate for pedestrian alarm rates was no more than 1:10 000.

Estimates of vehicular traffic proved more problematic, as the only data available related to traffic at sea ports. It was considered that the freight at sea ports would be significantly different to that entering a major sporting event and so an estimate of 1:1 000 was assumed, this figure was to incorporate both nuisance alarms and false alarms.

6.3 Solution

Initially two solutions for pedestrian screening were trialled, both offering different advantages and disadvantages in terms of layout, performance, ease of operation and cost. The results were presented to the stakeholders for the final decision.

The chosen solution involved a three-tier system where there would be an initial screening to alert the operators of an incoming source of radiation. This was carried out with a 4 litre NaI(Tl) in a fixed pillar with associated hardware and software and connected to a site wide network. Data was sent to the detection experts based at the Park Operations Centre (POC) indicating the isotope identified and dose rate.

The second stage involved localising the source where selected visitors were isolated from the main queue and the individual or bag would be identified. Coarse localisation (~10 people) was provided by a PVT-based portal monitor. Fine localisation (one individual/bag) was carried out with a combination of a pager type detector and an under conveyor monitor placed at the exit of the baggage x-ray scanner.

The third stage was to identify the isotope emitting the radiation using a hand-held radioisotope identification device (RID). The RID could be connected to a network-attached laptop in order to relay the spectrum and the result of the analysis to the detection experts at the POC. This final screening also provided an opportunity to interview the individual in order to establish the reason for the alarm.

By combining the information from all detectors with the outcome of the interview it was possible to establish the cause of the alarm with a good level of certainty on every occasion.

One vehicle system was trialled using fixed PVT portals for primary screening with RIDs for secondary screening.

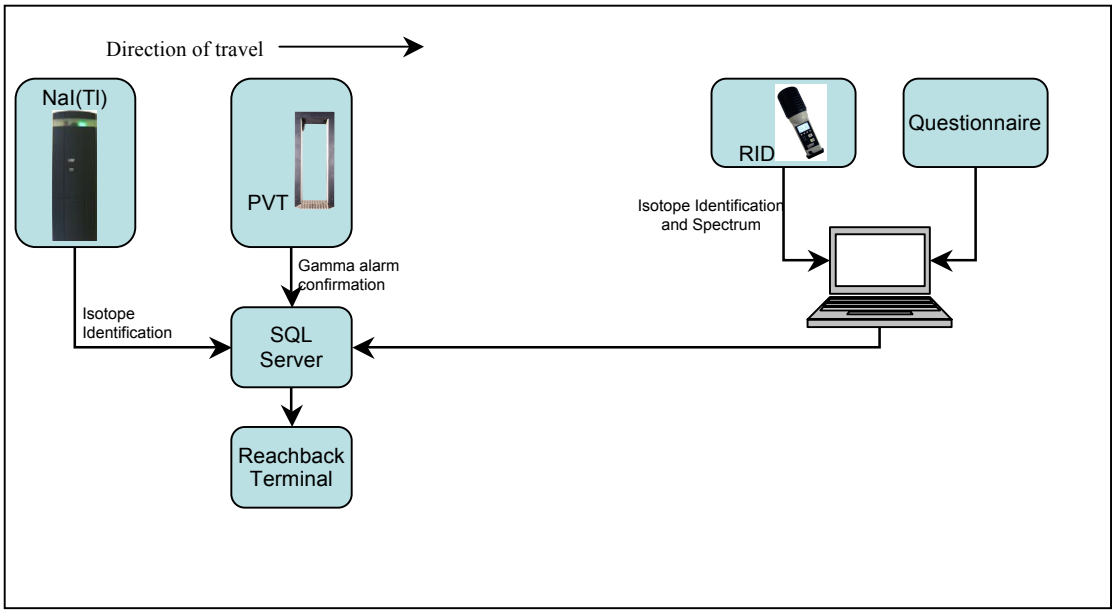

Figure 6.1 Detection system at the London Olympics.

6.4 Reachback

Data from all instruments were sent back to the POC, which was manned continuously throughout the games. All data was stored in an SQL server database with custom displays to present the alarm status for all instruments. Instrument status notifications included 'OK', 'fault', 'disconnected' and 'alarm'.

Pedestrian systems would initially show an alarm and the isotope identified but not the spectrum acquired. As the incident developed other alarms were triggered and additional data was made available. This data was triaged at the POC, with two instruments providing identification. In order to counter the possibility of there being a conflict in the identification results of both instruments the spectra could be further examined by detection experts using additional independent analysis software. Should there be any further doubt then the spectra could be sent to AWE for further in-depth analysis.

6.5 Lessons learned

There were many technical issues as a result of the limited timescale for the project. The project was initialised in early 2011 with the opening ceremony on 27 July 2012. This allowed little time from project initiation to completion. One of the first problems to overcome was the urgency in making the decision regarding the equipment to be used. With a project of this size there were going to be long lead times for the manufacture of monitors and in particular the detector crystals. This highlighted the need to get a plan developed as soon as possible.

The constant building of the park infrastructure severely limited the time available for installation, and plans for the site layout constantly changed, further compounding this problem.

On-site testing was further hampered by an unstable power supply, which continued for several weeks. It was therefore important to find alternative options for testing the

equipment and procedures off site. The aim of testing was to demonstrate end-to-end system functionality incorporating the radiation detection portals, vehicle/pedestrian management system, handheld detectors, networking, reachback workstation and operational procedures.

A live test event was arranged for November 2011 during the handball/goalball events, where 50 000 spectators attended. This event highlighted some technical issues including networking dropouts, portals triggering alarms when there was an extended occupancy and poor visibility of the remote displays in bright sunlight.

Final on-site testing to the required standard was not possible due to the power problems and other work at the entrance lanes. This testing could have eliminated some of the problems with instrument setup during the lead up to the games where there were a number of false alarms; the manufacturers and the suppliers worked hard to resolve these issues in time for the opening ceremony but would have benefitted from additional testing time. As a result of this limited testing time one vehicle monitor appeared to have a faulty detector which caused a small number of false alarms. The monitor was situated in a busy lane where access for service engineers was limited and therefore it was not possible to rectify the issue in time. Due to the distinct way in which this monitor generated alarms the monitor remained in service throughout the games with the fault unresolved.

Pedestrian portal monitors occasionally showed ‘out of service’ when the queues were busy. This was caused by occupancy sensors being constantly set by people standing in the portal. The portal monitor did not send a signal to reachback while occupied and so the reachback system assumed the monitor was faulty. The matter was resolved by working with security staff to ensure that the monitors were kept clear at all times.

Every isotope identified by the pillar type detector was confirmed by the RID. This provided the detection experts at the park with greater confidence in the systems as the games progressed.

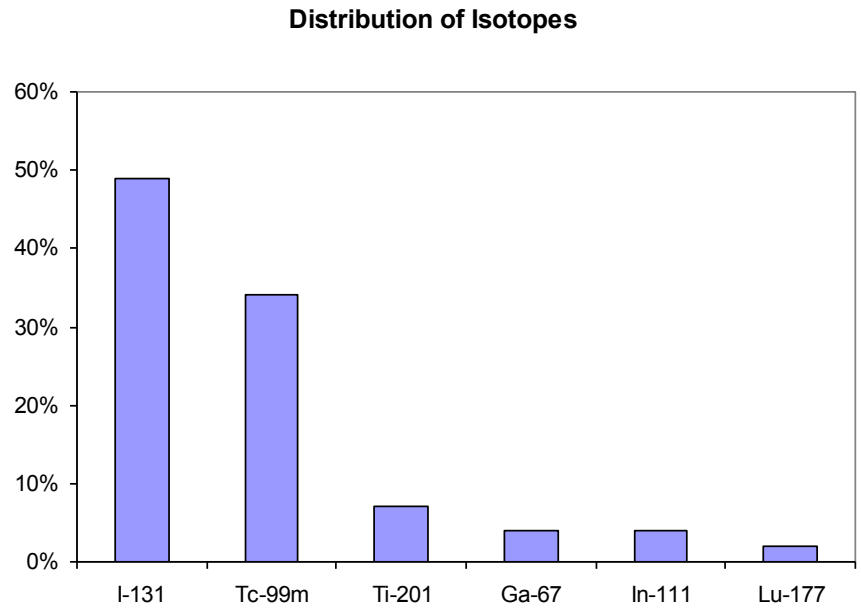

Figure 6.2. Isotope detected (95 alarms).

6.6 Outcomes

Pedestrian systems

There were 2.6 million visitors to the park screened; this figure excludes staff and athletes. There were a total of 95 alarms, all generated by persons having had medical treatment with radioisotopes. The alarm rate was approximately 1:27 000; 91 % of all alarms were generated by three isotopes, ^{131}I = 49 %, ^{99m}Tc = 35 % and ^{201}Tl = 7 %.

Vehicles

Approximately 10 000 vehicles were screened and there were 144 alarms; 63 % of those were caused by the one faulty system in a single day before the opening ceremony. The isotopes identified were ^{40}K, ^{226}Ra, ^{232}Th and ^{238}U, which were all typical of background measurements in that area.

7 Radiological and Nuclear Systems and Measures for 2010 Vancouver Winter Olympics

Weihua Zhang, HC

In 2010, Canada hosted the winter Olympic Games ('the games') in Vancouver and Whistler, British Columbia. This was the largest sporting event ever undertaken in Canada. Security and public safety were major considerations in the planning and conduct of the games. The Royal Canadian Mounted Police (RCMP) was identified as the lead agency responsible for the development and delivery of games security and public safety (GS&PS) [RCM, 2012].

In December 2008, the government of Canada approved a request from the RCMP's National CBRNE Response Team ('the national team') for chemical and radiological scientific support prior to and during the games. Biological scientific support had been integrated with the national team for years; the addition of chemical and radiological capabilities provided an unprecedented degree of technical support and reachback across the CBRNE spectrum. Assets for surveillance, analysis and scientific advice were deployed to Vancouver and Whistler and set up in 'science towns,' which were co-located with operational bases for the games' CBRNE tactical teams. For radiological and nuclear support, additional measures were implemented to enable reachback to staff at their labs and offices in Ottawa, approximately 3 500 km away [QUA, 2010].

RN detection equipment, analysis tools and subject-matter experts were drawn from radiation groups that exist within the Canadian Department of National Defence, Natural Resources Canada and Health Canada. These organisations regularly collaborate on projects related to nuclear emergency preparedness and counter-terrorism research. The history of operational science for the games is elaborated in [DRD, 2010]. For the games, they operated collectively as the Federal Radiological Assessment Team (FRAT).

The FRAT/science town model recognised that Canadian scientists were not trained to enter environments containing hazards that were either unknown or outside their areas of specialisation. Therefore, tactical CBRNE security teams (made up of first responders) were equipped and trained to collect data or physical samples from inside a 'hot zone' and send it to subject-matter experts off site. The FRAT team lead, called the scientific advisor, served as the bridge between tactical command and scientific assets, which included specialists in radiation monitoring and spectral analysis, environmental sampling and analysis, and radiation protection.

The main tasks to prepare for the games included advice to RCMP regarding RN surveillance strategies and equipment, equipment procurement and networking/data transmission: set up and testing; background characterisation; planning and protocol development; training and exercising; and logistics. During the event, a variety of monitoring strategies were used for discreet surveillance, and procedures were in place to investigate and respond to anomalous events (such as alarms) quickly and appropriately. CBRNE security in Vancouver and Whistler each had direct, 24/7 access to a FRAT scientific advisor who, in turn, could immediately activate FRAT resources, mobile spectroscopic survey systems and portable analytical labs.

Additional equipment and reachback to specialists in Ottawa were available on short notice throughout the games, and were actively engaged for the highest-profile events, such as the opening ceremonies.

7.1 Discreet Radiation Surveillance Technologies

Personal radiation detectors

Personal radiation detectors (hand-held dosimeters) were used for applications where a large number of relatively simple instruments were required. For example, these were provided to frontline security staff at strategic entry points to augment fixed-point detectors (see below). Users were given instructions on how to contact CBRNE tactical teams in the event that their equipment alarmed and how to manage the situation while they waited for reachback to review the fixed-point spectra and a tactical team to arrive. Police officers conducting venue sweeps were also provided with these detectors, while specialists were on stand-by to follow up in the event of an alarm.

There were no false alarms reported during the games. The most notable innocent alarm occurred when an officer carried his personal detector into a portable toilet that had previously been used by a medical patient. The response worked according to protocol, the CBRNE tactical team was called and dispatched to the site, the FRAT scientific advisor was notified, and spectra were quickly gathered and identified as ^{99m}Tc.

Backpack detectors

Portable backpack detectors [TOI, 2010] were not included in the official surveillance plans for the games; however, they were deployed on a trial basis for two events. These systems are capable of detecting the presence of both neutron- and gamma-ray-emitting radionuclides, and can provide real-time full spectroscopic relay of data every 2 seconds, displayed as a waterfall plot to facilitate detecting small radiation anomalies. For the games, personnel carried the backpacks in the crowds near chokepoints and data was transmitted to Ottawa and monitored in real time, remotely. When an anomalous signal was detected, an alarm was triggered simultaneously for the backpack carrier and the specialists in Ottawa. Analysis and notification of the scientific advisor was done from Ottawa. All alarms were innocent (medical patients).

Vehicle-borne detectors

Background mapping of Vancouver and Whistler, including all venues, was completed prior to the games using aerial, vehicle-borne and human portable systems. Mobile surveys were also carried out periodically during the games, and data was both reviewed on site and sent to Ottawa. Again, only innocent alarms occurred, the most interesting of which involved a barely detectable, anomalous signal identified by the reachback team from a survey done on a university campus. Further investigation with a directional, spectroscopic detector eventually revealed that the signal was coming from a core sample in a nearby geology laboratory.

Fixed-point detectors

Fixed-point detectors [ZHA, 2013] were strategically located at chokepoints where other types of screening were taking place. The units had no display and there was no on-site indication of an alarm; everything was monitored remotely. The detectors allowed for quick installation and tear-down (15 minutes). ‘Smart’ alarms were based on gross count and isotope identification. The system has built in state-of-health monitoring (SOH) and self-repair function. The SOH alarms can go to team members in Ottawa during off-duty

hours. Monitoring data can be remotely accessible and always available to fixed-point detector analysts and scientific advisors. However, post-event review of the data shows that some events (medical) were below set alarm levels in the noise range. To lower alarm levels, accurate identification is required at these low levels to differentiate medical versus potential threats and false alarm due to noise or rain events.

7.2 Operation of Technical Reachback Centre in Ottawa

All spectral data from backpack and detectors were organised into different time intervals and stored until they could be retrieved by modem or via the internet to the data centre located in Ottawa. The spectral data collected by the backpack detectors can be accessed from the data centre in real-time (every 2 seconds) and downloaded to a MySQL database, namely Linux System for Spectral Information (LINSSI), established under Linux [AAR, 2008, 2011], for the waterfall plot which can be used for detecting small radiation anomalies. An example is illustrated in Figure 7.1. A software package consisting of Unisampo/Shaman is used for peak energy and intensity determination, nuclide identification and activity calculation [UNG, 2007].

The fixed portal spectral data are downloaded every 15 minutes by a dialer programme and automatically processed into a Microsoft SQL database for storage. The spectral data analysis includes quantifying the amounts of total gamma dose-rate attributed to several isotopes automatically by a combination of software supplied by the vendors along with additional software developed in-house by HC. Another important advantage of reachback centre is to provide on-site specialist support in spectrometer calibration using well-shaped and well-known peaks in spectrum of naturally occurring nuclides. This is particularly important for daily analysis to prevent electronics drift caused by the channel-to-energy parameter error and poor peak fitting, as well as to verify experimentally derived coefficients determined by standard calibration sources in the laboratory.

7.3 Lessons Learned and Conclusions

Based on successes and lessons learned from the games, the Canadian RN community of practice has identified the following critical parameters for a sustainable reachback system.

Information sharing

A national reachback system needs to ensure effective collaboration/cooperation with relevant organisations (federal, internal) for information sharing of the experienced cases and for researching new instrumentation, analysis techniques, software and databases.

Quality system

An overall quality system is required in which all procedures are developed, validated and reviewed.

Training

Proper training is essential, and must be performed on a regular basis. This includes:

- operational training for scientific and technical specialists, including regular scenario training to practice responding in a realistic environment;
- joint training between security personnel (e.g. police) and scientists, including awareness training for both groups on the other's mission, objectives, requirements and constraints.

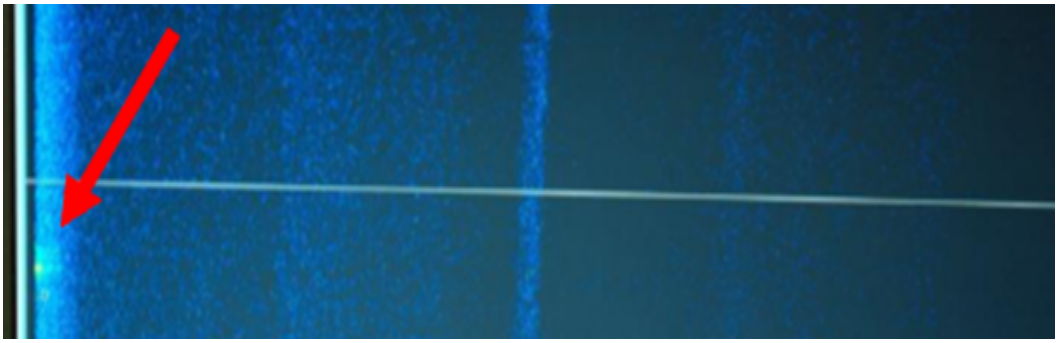

Figure 7.1. Anomalous reading (Tc-99m) identified during a survey using waterfall plot at reachback centre.

Data management

Very high priority should be given to data management and exchange protocols/formats as a basis for using scarce resources on a reachback basis.

Case studies

Interesting RN detection case studies, including both genuine anomalies and simulations, must be documented, shared and used in training and exercises.

Communication

Communication and information transmission routes between the involved organisations should be well established. The information release must be conducted in a proper manner, especially when dedicated to the public.

Legal framework

Including the reachback system in a national or regional legal framework would be an added value to the nuclear security legislation in force (preparedness/response plan to an RN incident). The responsibilities for the reachback system among those of other national organisations/agencies must be well defined.

Validation

The operation of a reachback must be validated, tested and reviewed. The support requested by the frontline operators to the reachback event must be well defined. Those details must be submitted on a developed, tested and reviewed template. That template must contain the necessary information to allow the reachback analysts to carry their duty in the allocated time.

Reachback/triage

For site specification, radiation specific triage should be designed with triage samples via additional testing for other threats to characterise an incident and to establish safe perimeters. Triage of the situation based on the actual measurements should also be carried out in a well-defined and commonly approved manner, possibly based upon support from state-of-the-art software.

Metadata

Gamma-ray spectrometry and neutron counting are the most important RN analysis methods suited for the reachback system. Therefore, details of the measurement conditions including the instrumentation and their settings must be indicated in the reachback request.

Timeliness

The timing for the reachback support to be delivered has to comply with agreed deadlines.

Record keeping

The reachback must keep a record on experienced cases for their own use or for information sharing with other organisations in nuclear security such as enforcement or nuclear forensic services.

Resources

The prime authority in charge must ensure the high expertise of reachback analysts by providing the necessary resources (human and funding).

References

[AAR, 2008] Aarnio P.A., Ala-Heikkilä J., Isolankila A., Kuusi A., Moring M., Nikkinen M., Siiskonen T., Toivonen H., Ungar K., Zhang W., LINSSI: Database for gamma-ray spectrometry, Journal of Radioanalytical and Nuclear Chemistry, Vol. 276, No 3 (2008) 631–637.

[AAR 2011]. Aarnio P., Ala-Heikkilä J., Hoffman I., Ilander T., Klemola S., Mattila A., Antero Kuusi A., Moring M., Nikkinen M., Pelikan A., Ristkari S., Salonen T., Siiskonen T. Smolander P., Toivonen H., Ungar K., Vesterbacka K., Zhang W. 'LINSSI — SQL Database for Gamma-Ray Spectrometry Part I: Database, Version 2.3', Helsinki University of Technology Publications in Engineering Physics Report TKK-FA861 (2011). Available at http://linssi.hut.fi/linssi_23.pdf.

[DRD, 2010]. Defense Research and Development Canada (DRDC) — Centre for Security Science, Public Security S&T Summer Symposium, June, 2010, Ottawa, Ontario, Canada.
http://publications.gc.ca/collections/collection_2011/rddc-drdc/D66-4-2010-eng.pdf.

[RCM, 2012] RCMP report, Games Security and Public Safety for the Vancouver 2010 Olympic and Paralympic Games, October 2012.

[QUA, 2013] Quayle Debora, Ungar Kurt and Zhang Weihua, DRDC Centre for Security Science: Radiological -Nuclear Detection Architecture for V2010, presented at ERNCIP Radiological and Nuclear (RN) Threats to CITHEMATIC GROUP meeting, 2013, Ispra, Italy.

[TOI, 2010] Toivonen Harri, Vesterbacka Kaj, Pelikan Andreas, Mattila Aleksi, Karhunen Tero, LaBr3 Spectrometry for Environmental Monitoring, Proceedings of Third European IRPA Congress 2010.

[UNG, 2007] Ungar K., Zhang W., Aarnio P., Ala-Heikkilä J., Toivonen H., Siiskonen T., Isolankila A., Kuusi A., Moring M., Nikkinen M., Automation of analysis of airborne radionuclides observed in Canadian CTBT radiological monitoring networks using LINSSI, Journal of Radioanalytical and Nuclear Chemistry, Vol. 272, No 2 (2007) 285-291.

[ZHA, 2013] Zhang Weihua, Korpach Ed, Berg Rodney, Ungar Kurt, Testing of an automatic outdoor gamma ambient dose-rate surveillance system in Tokyo and its calibration using measured deposition after the Fukushima nuclear accident, Journal of Environmental Radioactivity 125 (2013) 93-98.

8 Discussion

Information sharing on a nuclear security event or emergency is of vital importance for a correct response by the authorities. The RN thematic group of ERNCIP has identified a potential approach to improve data exchange at the technical level, which is outlined in a report on remote expert support of field teams [TOI, 2014]. This report suggests that further standardisation on formats and protocols is needed for nuclear security, including data handling storage and related software.

The RN thematic group sent a questionnaire in summer 2015 to all EU Member States to collect their views on reachback, information sharing and the way forward [TOI, 2015]. The principle of information sharing was widely agreed but its implementation may be difficult. Another key finding was that not all European countries have identified the need of information sharing in a nuclear security event, or they suggest using mechanisms, such as EURDEP dose rate data exchange, designed for a major nuclear accident. The survey shows that there is room for an information awareness-raising campaign on nuclear security and on the importance to share relevant technical and non-technical information among the authorities which could seek international support on bilateral basis.

Major public events, such as political summits or large sports events, emphasise the role of efficient reachback and fast response. The analyses of the London and Vancouver Olympics show that the preparations have to be started early, and it is necessary to have a measurement history long before the actual event in order to avoid false alarms. A reachback centre is needed to handle the technical information flow and to provide a comprehensive analysis of the findings. Law enforcement combines processed knowledge with information alerts and other non-technical information to plan and execute response measures in a timely manner.

The case studies in this document on national radiological or nuclear reachback systems show that some countries have advanced detection technology and response plans to deal with nuclear security events of different kinds and scales. The comprehensive approach to nuclear security provides the capability to keep continuous track and history over the radiological and nuclear measures and events at their borders and critical infrastructures. This capability includes means for the detection of criminal activity which is the basis for efficient response measures to prevent the escalation of the event. On the other hand, there are many countries which do not have these capabilities, and are thus more vulnerable to nuclear security threats.

For the implementation of an efficient reachback system there is a strong need for standardising the data acquisition, storing, and the final distribution of the analysis results. Major nuclear powers take this activity very seriously, and have 24/7, all-year national services for information processing. The case studies of Finland and France show that efficient European reachback is manageable and technically possible on a country-wide basis. The case study on Denmark reveals that countries with limited reachback resources need an adequate and standardised technical information-sharing mechanism to aid their national capacities for analysis services in a precise and timely manner.

References

[TOI, 2014] Toivonen Harri, Reppenhagen Grim Per, Tengblad Olof, Keightley John, Paepen Jan, Abbas Kamel, Schneider Frank, Nilsson Jonas, Peräjärvi Kari. Remote expert support of field teams, Reachback services for nuclear security. ISBN 978-92-79-45418-9, ISSN 1831-9424, doi:10.2788/20613. Luxembourg: Publications Office of the European Union, 2014. https://erncip-project.jrc.ec.europa.eu/download-area/category/7-radiological-and-nuclear-threats.

[TOI, 2015] Toivonen Harri, Reppenhagen Grim Per, Schoech Hubert, Keightley John, Tengblad Olof, Schneider Frank, Forsberg Carl-Johan, Peräjärvi Kari. Information Sharing in a Nuclear Security Event. Consultation of EU Member States on the Report 'Remote Expert Support of Field Teams; Reachback Services for Nuclear Security. JRC, ERNCIP. To be published.

LB-NA-27626-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/718077

ISBN 978-92-79-54066-0