Remote expert support of field teams

Reachback services for nuclear security
Task 2 deliverable 1

Harri Toivonen, STUK — Finland
Per Reppenhagen Grim, DEMA — Denmark
Olof Tengblad, CISC — Spain
John Keightley, NPL — United Kingdom
Jan Paepen, European Commission
Kamel Abbas, European Commission
Frank Schneider, Fraunhofer Institute — Germany
Jonas Nilsson, Lund University — Sweden
Kari Peräjärvi, STUK — Finland

2014

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.

Report EUR 27099 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 721, 21027 Ispra (VA), Italy
E-mail: erncip-office@jrc.ec.europa.eu
Tel.: +39 0332786045
Fax: +39 0332785469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC94535

EUR 27099 EN

ISBN 978-92-79-45418-9

ISSN 1831-9424

doi:10.2788/20613

Luxembourg: Publications Office of the European Union, 2014

Printed in Italy

ERNCIP thematic group for radiological and nuclear threats to critical infrastructure

Remote expert support of field teams

Reachback services for nuclear security

December 2014

Kari Peräjärvi, STUK, Finland — Coordinator of the task group
Harri Toivonen, STUK, Finland — Lead scientist for the development of this report

Other main contributors to the report

Per Reppenhagen Grim	DEMA	Denmark
Olof Tengblad	CSIC	Spain
John Keightley	NPL	United Kingdom
Jan Paepen	JRC-IRMM	EC
Kamel Abbas	JRC-Ispra	EC
Frank Schneider	Fraunhofer FKIE Institute	Germany
Jonas Nilsson	Lund University	Sweden

Experts who also attended the reachback meetings

Hubert Schoech	CEA	France
Magnus Gårdestig	Linköping University	Sweden
Bastian Gaspers	Fraunhofer FKIE Institute	Germany
Jolien van Zetten	NEN	Netherlands
Sakari Ihantola	University of Oxford	United Kingdom
Leticia Pibida	NIST	United States
Weihua Zang	HC	Canada
Christer Pursiainen	ERNCIP Office	EC
Peter Gattinesi	ERNCIP Office	EC
Aikaterini Poustourli	ERNCIP Office	EC
Carl-Johan Forsberg	ERNCIP Office	EC

Related ERNCIP documents:

1. List-mode data acquisition based on digital electronics, EUR 26715.
2. Critical parameters and performance tests for the evaluation of digital data acquisition hardware, EUR 26976.
3. Critical parameters and performance tests for the evaluation of list mode data files and analysis software. In preparation.
4. National reachback systems for nuclear security. In preparation.
5. Analysis of current state-of-the-art of knowledge and expertise in remote controlled radiation measurements and sampling using unmanned vehicles. In preparation.

Executive summary

Strengthening chemical, biological, radiological, nuclear and explosive (CBRNE) security in the European Union (EU) reduces the threat of and damage from CBRNE incidents. One of the main issues facing the EU security industry is its highly fragmented nature, exhibiting a lack of standardisation and of harmonised certification procedures. The need for standardised information sharing between competent authorities and international bodies regarding radiation measurements and data analysis has been recognised by several experts in response to Commission mandate M/487 for the establishment of European security standards. This report will suggest a way forward to develop protocols for more efficient cooperation between competent authorities and remote expert support or reachback centres at the national and international level.

Not all EU Member States have the capabilities to process data provided by nuclear security instruments, and thus should consider instigating a coordinated capability yielding a more efficient and comprehensive approach in responding to future nuclear emergencies. This could be achieved by reachback centres across Europe (built upon existing national facilities and expertise) and would provide analysis services for alarm adjudication. Efficient data sharing and processing across EU Member States requires the use of standard data formats and protocols.

The radioactive and nuclear materials (RN) thematic group of the European Reference Network for Critical Infrastructure Protection (ERNCIP) launched an initiative in 2014 to develop a standard list-mode digital data format for nuclear instrumentation, under the auspices of the International Electrotechnical Commission (IEC). Similarly, there is a need to improve standardisation at the data management level, requiring a technical standard for data handling protocols, which may be a non-trivial effort. For spectrometric data, no such protocol has been defined at the international level. The RN thematic group therefore proposes to develop a European standard for data storage protocols on nuclear and radiological data exchange, particularly with regards to reachback.

National nuclear security regimes involve frontline officers operating detection instruments at borders or other critical sites. Although skilled at the operation of the instruments and procedures for response to a nuclear security event, they are typically non-experts on radiation detection. When an instrument alarm or an information alert is triggered, standard response procedures, including dedicated measurements, may need to be conducted for assessment of the event. The operator or frontline officer may not be able to interpret the results of the instrument and consequently would require timely support from experts, which could be provided using reachback centres.

A reachback system is of vital importance not only for nuclear security, but it also improves the effectiveness and efficiency of missions regarding emergency response, nuclear safety, safeguards and environmental monitoring. Technically this is provided remotely via data exchange between frontline officers and off-site experts.

There are two related standards that are intended to define the data format (extensible markup language (XML)) produced by radiation detection instruments: IEC 62755 and American National Standards Institute (ANSI)/ Institute of Electrical and Electronics Engineers (IEEE) N42.42 ([1]). However, these standards do not address the benefits associated with modern and powerful data acquisition methods (list-mode).

The purpose of standard data formats is to facilitate manufacturer-independent transfer of data and information from radiation measurement instruments to the analysis resources which could be located on-site or far away in a reachback centre. Complementary to standard data formats there is a need for standard procedures to handle the information within the formats.

Development of a protocol into a technical standard may constitute a significant effort, since communication and data processing systems vary, including computer security solutions. However, common data structures within data processing systems would enable more efficient and sustainable information sharing. The obvious choice for these common data structures is a standard database which all stakeholders would have in their own custody.

The database creates a solid foundation for the communication of data, analysis results and advice in various phases of the detection and alarm adjudication process. All software processes must obey the rules of the database, including acknowledgement of certain reserved words. The advantages of a data handling protocol, based on a standard database, are as follows.

- Efficient interoperability becomes possible between competent authorities and Member States.
- Data and information provided by the instrument grow to knowledge through expert analysis (via reachback).
- The changes needed to be made in existing data acquisition systems are minimal.
- Remote analysis capability may change the way the instruments operate in the future. Instead of local analysis, the data are processed at a remote server and the results are returned in real time via cell phone, e-mail or web page.
- A rapid response can be achieved with less manpower.

The open-source database Linssi is used for data storage in many institutions, for example in Finland (*Säteilyturvakeskus* (STUK)), France (Institute for Radiological Protection and Nuclear Safety (ISRN)), Canada (Health Canada (HC)), Germany (*Bundesamt für Strahlenschutz* (BfS)) and Ukraine (State Scientific and Technical Centre for Nuclear and Radiation Safety (SSTC NRS)). Linssi defines implicitly a protocol defining data handling, as well as information and knowledge created in various phases of the detection and alarm adjudication processes. All users communicate with the database, rather than directly with each other. The starting point of the work for defining a common data structure could be the database Linssi. In addition, the new system should be designed to incorporate list-mode data.

([1]) IEC 62755 is adopted from ANSI/IEEE N42.42.

Contents

Acronyms

BfS	*Bundesamt für Strahlenschutz*, Germany
BRD	backpack radiation detector
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
CSIC	Spanish national research council
DEMA	Danish Emergency Management Agency
EDA	European Defence Agency
ERNCIP	European Reference Network for Critical Infrastructure Protection
HC	Health Canada
IAEA	International Atomic Energy Agency
IND	improvised nuclear device
IRSN	Institute for Radiological Protection and Nuclear Safety, French national public expert in nuclear and radiological risks
JRC	Joint Research Centre, the European Commission's in-house science service
LHC	Large Hadron Collider
Linssi	LINux System for Spectral Information, open-source database
LML	Linssi Markup Language (XML)
MORC	material out of regulatory control
NaI	Sodium iodide, scintillator crystal used in gamma spectrometer
NATO	North Atlantic Treaty Organisation
NEN	*Netherland Standardization Institute*
NIST	National Institute of Standards and Technology, United States
NORM	naturally occurring radioactive material
NPL	National Physical Laboratory, United Kingdom
NSDA	nuclear security detection architecture
PRD	personal radiation detector
RDD	radiological dispersal device
RED	radiation exposure device
RID	radionuclide identification detector
RN	radioactive and nuclear materials
RPM	radiation portal monitor
SPRD	spectroscopy-based personal radiation detector
SRPM	spectroscopy-based radiation portal monitor
SQL	Structured Query Language
SSTC-NRC	State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine
STUK	*Säteilyturvakeskus*, radiation and nuclear safety authority, Finland
WLCG	Worldwide LHC computing grid
XML	Extensible Markup Language

1. Introduction

Nuclear security often involves frontline officers or first responders operating detection instruments which are large volume, high-efficiency detectors. If anomalous radioactivity is detected, secondary measurements are conducted, or should be conducted, with gamma spectrometers or neutron detectors. However, an expert may be required to interpret the findings. The expert would either arrive at the scene equipped with specialised instruments, or a sample would be collected and sent off-site for further analysis.

A more recent development is the direct use of detectors along with data sent wirelessly or via dedicated networks to an off-site analysis centre, where the experts follow the measurements in real time and provide advice accordingly. This approach provides a faster and more reliable response and requires fewer human resources. Real-time transmission of data to subject matter experts enables a focus on the core activity of the field mission: to provide correct analysis and enable justified decision-making. The analysis centres return key findings in a format suitable for the field operation. This process is called remote expert support or reachback. Sometimes the word ‘triage’ is used in the same context (France, United States).

Transferring data is efficient, safe and fast compared with the movement of experts and samples. The new technology is especially useful in nuclear security and in crisis management, when time and resources are scarce and increased analysis capacity is required. In order to utilise the opportunities opened by these new technologies, the detection systems have to be interoperable so that the data from each type of detector can be easily analysed by different analysis centres. Various international and national data formats have been developed for efficient spectral data transfer. Modern data formats provide key information wrapped around metadata (tags) which describe the source of the information. This kind of information is easy to parse for further processing via the application software.

Recent developments in digital radiation detection systems are based on list-mode data collection (time-stamped event-data). The new technology will improve detection and source localisation capabilities [KEI, 2014] [PAE, 2014]. However, list-mode data create new challenges for the data management. The spectrum is no longer the basic entity of the data collection; the spectrum is, in fact, the very first analysis result, although of basic or primitive nature.

The list-mode data have to be in a binary format to allow fast processing of millions of events provided by the detection system. The binary list-mode format is efficient in a variety of applications, including direct in-field measurements, analysis of samples in a laboratory or even complex detection systems containing several detectors. The data management must be able to handle all information regarding the mission or the measurement. This means that the data acquisition systems must provide binary files (lists of events, such as time stamps and pulse heights) and metadata simultaneously. These two types of data have to be interlinked with a common identifier in both data structures.

Successful interoperability of the systems requires that European and international standards are devised for the data format. The need for standardisation of list-mode data has been recognised by several experts in response to Commission mandate M/487 for the establishment of European security standards. The European Standards organizations *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).

The work has been allocated to CEN/TC 391 'Societal and Citizen Security' whose secretariat is provided by the *Netherland Standardization Institute (NEN*). CEN/TC 391 investigated with several industry players and public authorities the priorities for future standardisation activities in three security thematic areas set out in the European Commission Action Plan for innovative and competitive security industry [EC 2012]:

1. Chemical, biological, radiological, nuclear and explosives (CBRN-E).
2. Border security — automated border control systems (ABC), as well as biometric identifiers.
3. Crisis management and civil protection — including communication and organisational interoperability.

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. In short, the focus of the RN thematic group is to advise CEN/CENELEC on standardising formats and protocols used in sending the collected data to enable further analysis. The issue 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 works with the following three issues.

1. List-mode data acquisition based on digital electronics. Time-stamped list-mode data format produces significant added value compared to the more conventional spectrum data format. It improves source localisation, allows signal-to-noise optimisation, 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 singles gamma and ultraviolet (UV)-gated gamma spectrometry.

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 accidents, dirty bombs before and after explosion, search for nuclear and other radioactive material out of regulatory control.

([2]) The (IPSC) of the European Commission's Joint Research Centre. The Institute provides scientific and technological support to EU policies in different areas, including global stability and security, crisis management, maritime and fisheries policies and the protection of critical infrastructures. IPSC works in close collaboration with research centres, universities, private companies and international organisations in a concerted effort to develop research-based solutions for the security and protection of citizens. The ERNCIP mission is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. The ERNCIP office has been mandated by the Directorate-General for Migration and Home Affairs (DG Migration and Home Affairs) of the European Commission.

This report describes the reachback rational in the context of nuclear security. The report deals with remote expert support (item 2 on the previous list) and suggests a way forward to develop protocols for more efficient cooperation between competent authorities and reachback centres at the national and international level.

2. Reachback

Nuclear security regimes involve frontline officers operating detection instruments at borders or other critical sites. Frontline officers are usually non-experts on radiation detection although they attend training on regular basis for the operation of the instruments, including procedures for response in a nuclear security event.

The detection instruments could be fixed, such as radiation portals monitors, or mobile equipment which are able to detect gamma radiation or neutrons. In some cases mobile laboratories are deployed; a vehicle can be equipped with sophisticated sensors and communication assets. In addition, unmanned detection systems (robotics) are increasingly used for measurements where human life could be in danger.

In a nuclear security event an instrument alarm or an information alert is triggered and then standard operation procedures are applied. Dedicated measurements may have to be conducted to confirm the finding. However, when an alarm is confirmed, the operator or the officer may not be able to interpret the results of the instrument. Therefore, management of the event is difficult. Support from the experts is required, i.e., technical reachback support would be needed.

2.1. From raw data through information to wisdom

To conceptualise the nuclear security measurement process (and related data processing leading to initiation of an appropriate response) it is important to differentiate between raw data, data, information, knowledge and wisdom, including messaging and perception of the results [ACK, 1989]. For definition of the categorisation of these terms, see Appendix 1.

Nuclear security measures deal with the following products.

1.	Raw data	Time stamped events detected by instruments**.**
2.	Data	Spectra generated from raw data at certain intervals.
3.	Information	Messages (metadata, data, raw data, initial analysis results) in compact format.
4.	Knowledge	Verified information consisting of nuclide identification, activity and age estimation, device diagnostics, etc.
5.	Wisdom	Appropriate decision-making based on the attained knowledge. A message which is useful for the frontline officers or first responders to interdict.

Items 2 and 3 refer to field operation (item 1 is a future enlargement) whereas correctly balanced response requires expert support (reachback), i.e. items 2 to 4. However, they all are connected through various messages which are information. Item 5 is the final information product for the implementation of response, and its jurisdiction belongs to the operations centre.

The concept of information is used in different ways depending on context and culture. Information is closely related to other items, such as communication, data, instruction, knowledge, meaning, understanding, perception and representation. In nuclear security it is very important to differentiate between information and knowledge. Wisdom refers to adjudication which combines technical and non-technical factors to clarify the threat or resolve the alarm.

There is considerable overlap or confusion regarding terminology in different concepts of operation. In some cases the technical reachback centre may handle only knowledge whereas wisdom is formed in the operations centre. In a simple scenario, all decisions are made in the field based on the information available locally.

2.2. Comprehensive reachback support to field operations

The cooperation between field operators and experts must be straightforward, yet effective. In a larger, nationwide or international perspective, such as cross-border control or large-scale contamination, complexity increases due to different systematic approaches, regulatory procedures, instrumentation or documentation which mainly lead to different concepts of operations and reachback systems. This calls for uniform reachback systems, at least in the European context, to enhance cooperation between countries.

The concept of reachback has different meanings depending on the context. Reachback is used in the United States Department of Defense as the process of obtaining products, services, applications, forces, equipment or material from organisations that are not deployed [DIC, 2010].

In the ERNCIP context, the RN thematic group has mainly dealt with data and information, and they are handled from the point of view of spectrum analysis and alarm adjudication which is the main focus of the present report. However, we will here take a comprehensive effort analysing remote support of field operation in general.

Field operators mainly focus on actions to prevent harm to the public. During their operations they have many concerns to be dealt with. The most important one being: how to perform reliable and fast measurements safely?

The correct procedures must be developed and taught, but they are widely dependant on the available instruments and their limitations. Field operators normally only have basic training, or slightly beyond basic knowledge, to use the instruments, which in a complex environment requires online expert guidance.

A vital component of reachback systems is the communication between expert(s) and field operator(s). Communication procedures must enable an acceptable level of understanding. The communication system itself must be reliable (robust) and redundant with some diversity. The off-site reachback experts on the other hand require rapid analysis and guidance tools to give precise advice and response to field operators.

Radiation measurement instruments are exposed to different conditions when performed in a laboratory or outdoors. In a laboratory, there may be complex setups in a controlled environment with constant temperature, humidity and no wind or other kind of noise or disturbance factors. Hence accurate measurements can be performed with highly reliable and calibrated instruments. In the field the setup is expected to be complex. Temperature changes can make the instrument calibration drift; humidity can influence calculation of beta activities; strong sources can make the finding of weaker

sources placed nearby extremely difficult; and the complexity of the environment can create several limitations to the plan of action. To take all factors into consideration and find ample solutions is not always possible, but without the help of the reachback this might be impossible.

The technical role of the field operator is to provide rapid measurements for the expert and execute safety and security operations to protect the public. Response measures, including mitigating actions, such as regulating public behaviour through advice, recommendations or evacuation, have to be based on correct information and knowledge. Therefore, the quality and speed of measurements, and their correct analyses, are vital.

2.3. Application-driven services

The reachback centres provide different services, depending on national best practices and concept of operations. The following is a list reflecting the state-of-the-art, but it is by no means exhaustive.

2.3.1. Analysis of spectra of interest

When an alarm is triggered, frontline officers or other responders send their key data to experts, either directly or via a coordinating organisation which is in touch with all key players related to the event. The technical reachback centre has wide expertise in spectrum analysis, including the capability to handle various data formats, calibrations, peak search and identification of radionuclides. The experts either confirm or reject the initial alarm. The experts may also provide more detailed information, such as the following.

- Activity estimation (measurement geometry must be available).
- Shield analysis (spectrum baseline tells about the surroundings of the source).
- Presence of nuclear material or devices (improvised nuclear device (IND), neutrons, plutonium, uranium, isotope ratios).
- Crime scene management (advice on sampling, safety issues).

Some national reachback centres are able to perform these tasks 24 hours a day, 7 days a week (24/7). A set of data is required from the field instruments for the analysis which will resolve the situation.

2.3.2. Participation in law enforcement field operations

Via reachback services a radionuclide expert is deployed virtually to the field for the search of radioactive material, analysis of the acquired spectra or to identify any safety issues. This kind of operation may be extremely powerful as the frontline officers might be able to understand the nature of the findings immediately. Certain threat scenarios may involve diversions/distractions or ‘red herrings’ that are intended to mask the real intentions or targets. In these cases, it is important to resolve the findings quickly, mark the site and continue the operation. Expert support provided by the reachback is vital for the success. This kind of concept of operation is implemented by the Finnish police in cooperation with the Radiation and Nuclear Safety Authority (STUK).

2.3.3. Reanalysis of border monitoring data in real time

The border monitoring instruments are independent systems, which provide an alarm along with a reason for it. Unfortunately, automated nuclide identification is not always reliable and may generate many false alarms, unless special arrangements are available. Usually these arrangements are part of the overall concept of operation. A common solution is to perform secondary measurements via spectrometers, but this procedure may demand too many resources.

A large airfield or harbour could have tens, or even hundreds, of detection instruments. The daily data volume can be enormous depending on the concept of operation. The fraction of false alarms could be large (rate of 10^{-3}–10^{-6}) giving a few, or even hundreds of alarms per day for a large detector system reporting every second. The upper range refers typically to counters (plastic detectors) whereas the lower limit can be reached with spectrometers. The alarm rate could be reduced by certain specific means, such as requiring multiple detections from one instrument or using occupancy sensors (accept alarm only if the target of interest is in the measurement position). However, daily false alarms may still be unacceptable, and further measures have to be taken to reduce this irritating functionality without compromising the capability to detect actual threats.

One way of resolving these alarms is to reanalyse in a reachback centre all suspect spectra, including combining data from different detectors to allow a more comprehensive analysis. This, however, requires automated, real-time data transfer from the action site to a central database which is accessible to the reachback centre. High-quality automated analysis and data management algorithms have to be developed and implemented. In addition, the data processing software must also support efficient interactive analysis and review of the data and the results. This kind of concept of operation is implemented by Finnish customs in cooperation with STUK.

2.3.4. Advice to operation centres and other national authorities

For the success of a field mission, it is essential for the operations centre and other competent authorities to obtain advice from the experts to resolve unusual findings. Consequently various communication mechanisms must be available, including secure voice communication, text messages, e-mail and shared resources, such as dedicated secure cloud services.

2.3.5. Advanced support to special field operations

The reachback centre may provide special resources for the field operations. It could support local authorities by sending highly trained nuclear experts with high-resolution hardware and other advanced technology, such as gamma or neutron camera, sampling systems and methods for rendering safe a device or material (radiological dispersal device (RDD), radiation exposure device (RED), IND, contamination management). The deployment of the new assets should be based on threat and risk assessment [IAE, 2014].

2.3.6. In depth reports about the event

An essential service of the reachback centre is to provide timely reports on the event followed by a more detailed analysis at a later time. Some of the reports are intended for decision-makers; some are the basis for public communications; some are scientific analyses for future usage. Timely reporting is an enormous challenge and requires adequate resources. If all of the data are gathered in a database, automated reporting tools can be designed to cover part of the need. However, often these reports are intended for specialists only.

2.3.7. Emergency preparedness and readiness

To ensure a reliable nuclear security regime, emergency preparedness and readiness plans need to be developed at different local and national levels, including certain facilities and other critical infrastructure. Such plans are intended for a comprehensive response to a nuclear security event. They should be developed in collaboration with all stakeholders involved in nuclear security, in particular with police, customs, border guards, nuclear operators, civil authorities and regulators. Nuclear safety and security should be combined in these plans and they should also address the expert support to field teams.

2.4. Alarm adjudication in nuclear security

Alarm adjudication is a process which explains the cause of a detector alarm. This may be a complex process because in addition to threat-related alarms, there are false and innocent alarms [IAE, 2013].

1. False alarm — No nuclear or other radioactive material is present.
2. Innocent alarm — Radioactive material is present but does not exceed regulatory levels.

   Examples:

   - Cases where regulatory control is not applicable, such as items containing naturally occurring radioactive material (NORM).
   - People recently subjected to medical procedures involving radioactive material.
   - Controlled regulated materials, such as industrial devices incorporating radioactive material; these devices should have formal transport documents and appropriate package labelling.
3. Confirmed alarm. Nuclear or other radioactive material is present and the material is out of regulatory control (MORC). In this case, appropriate response measures should be initiated in accordance with the national response plan.

Deployment of detection instruments at borders, ports-of-entry and other checkpoints has two disparate priorities: (1) the reliable detection and characterisation of threat materials and (2) the rapid identification of non-threat materials without disturbing innocent people or legal transport of goods. This is a difficult process without subject matter experts, although advanced technology could be available at the site of detection. Therefore, the in-field radiological or nuclear operations should be connected to technical reachback services which can provide the expertise necessary for alarm adjudication. Without such support there will be an unacceptable number of response operations and delays from resolving alarms, or even worse, the true cause of the alarm will not be clarified. There must be established capabilities and procedures for the operators of the detection instruments to ‘reach back’ to trained analysts and appropriate subject matter experts [BUC, 2009].

Technical reachback services include on-call technical experts and other resources, such as advanced automated and interactive analysis software intended to give an immediate second look at the data received. Often these services are far away from the action site. For efficient response, reliable communication and especially standardised data formats and protocols are required.

2.5. Science and remote expert analysis of large amount of data

An example of a kind of expert analysis system from the academic world is the data handling at the Large Hadron Collider (LHC) ([3]) at the European Organisation for Nuclear Research (CERN). The system works in an analogous way with reachback centre design for national security. LHC is generating approximately one petabyte of raw data per second. None of today's computing systems are capable of recording at such rates. A fast electronic preselection of events (one out of 10 000 events accepted) is performed, but still over 25 petabytes per year is stored.

The data are aggregated at CERN, where initial data-reconstruction is performed, and a copy is archived for long-term tape storage. Another copy is sent to several large data centres around the world forming the Worldwide LHC Computing Grid (WLCG), which provides the resources to store, distribute, and process the data. WLCG combines the power of several hundreds of collaborating centres in 36 countries around the world. The WLCG collaboration performs more than 1.5 million analyses per day, corresponding to a single computer running for more than 600 years.

The grid is thus a network of computers, each of which can analyse a chunk of data on its own. Once a computer completes its analysis, it can send the information to a centralised computer and accept a new chunk of data.

The system is organised into tiers.

- **Tier 0** is CERN's computing system, which processes **raw data** and divides it into **data** for the other tiers.
- **Tier 1** sites (13) located in different countries ([4]) accept **data** from CERN over dedicated computer connections. These connections are able to transmit data at 10 gigabytes per second. The Tier 1 sites process the data, divide and send them further down the WLCG.
- **Tier 2** sites (>100) connect with the Tier 1 sites. Most of these sites are universities or scientific institutions. Each site has multiple computers available to process and analyse data using the **ROOT** framework (see Appendix 2) in order to obtain **information**.
- When each processing job is completed, the **Tier 2** sites push **knowledge** back up the tier system.

Any Tier 2 site can access any Tier 1 site in order to allow researchers the chance to focus on specific information.

One challenge with such a large network is data security. CERN determined that the network could not rely on firewalls because of the amount of data traffic. The system instead relies on **identification** and **authorisation** procedures to prevent unauthorised access to LHC data.

2.6. Military and reachback

The mission of a military reachback centre is to provide comprehensive consulting services for the basic operations, especially in deployment. Typically a single point of contact is arranged for CBRN matters. Then information flow is straightforward and the CBRN consultant in charge gets access to

([3]) How the Large Hadron Collider works. http://science.howstuffworks.com/science-vs-myth/everyday-myths/large-hadron-collider6.htm

([4]) http://home.web.cern.ch/about/computing/grid-system-tiers

relevant information quickly. For example, Germany is establishing a competence centre as part of the department of operations support (Division of deployment of the counter-CBRN command) within the new organisation of the Bundeswehr. Thus, the accessibility of necessary information can be guaranteed for all missions, especially for counteractions regarding CBRN events.

Counter-CBRN consulting requires highly qualified and specially trained personnel who must have a scientific background in physics, biology and chemistry to provide high-quality support through the evaluation of situations and the response to CBRN-related issues. Further, to evaluate CBRN risks and hazards in detail, personnel with medical, meteorological and geological training are required. If needed, experts from other organisations as well as civil experts are consulted.

The work programme of Horizon 2020, protecting freedom and security of Europe and its citizens 2014–15, expresses very clearly the need for cooperation between civilian and military efforts in security [HOR 2020] ([5]): 'Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes.' Therefore, when new technical solutions are envisaged for nuclear security, it is wise to consider civil and military needs simultaneously. One such common area of interest is reachback.

In the military domain the cooperation between different field troops is of vital importance. The principle of cooperation between different partners through common data structures has turned out to be powerful. One such military standard is allied tactical publication (ATP-45) developed by the North Atlantic Treaty Organisation (NATO) [NAT, 2010]. Furthermore, NATO has built a system called Majiic ([6]) which works at operational, architectural and technical standard levels for interoperability of a wide range of ISR assets. The idea is to use common interfaces for data exchange, keeping modifications to any given system very minor. The key principle is to upload data to a shared data server which gives services to all relevant partners, i.e. the users exchange data through the server, not directly with each other. The Majiic-shared database system enabled NATO to rapidly share full motion video in Afghanistan.

Majiic 2 is the successor of the successful Majiic project ([7]). Under the new program current technologies will be further developed and applied in a wider context, for example, in support of the civil authorities.

Majiic was initially designed for other types of sensors than those used in the CBRNE domain. However, this is not a limitation, as Majiic 2 can deal with any type of sensor and data.

([5]) http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1115-fct-03-2015.html

([6]) MAJIIC comes from multi-sensor aerospace-ground joint intelligence, surveillance and reconnaissance (ISR) interoperability coalition. http://www.nato.int/docu/update/2007/pdf/majic.pdf

([7]) NATO nations deepen cooperation on intelligence, surveillance and reconnaissance. http://www.nato.int/cps/en/SID-F3AF6544-59A62A26/natolive/news_71562.htm?selectedLocale=en

3. Reachback and nuclear security detection architecture

Nuclear security detection architecture (NSDA) should be designed in a holistic process, as defined by the International Atomic Energy Agency (IAEA). Reachback is only one component of the system, albeit an important crosscutting element of the detection architecture [IAE, 2012, 2013] [GIC, 2009]. Nuclear security is seen in a comprehensive way where information sharing plays the key role. Integrating application-specific technologies and operations makes cooperation possible between the authorities.

Nuclear security activities need to be nationally coordinated so that all activities are in agreement with national legislation, regulations and other provisions. The NSDA deals with threats related to nuclear (N) and other radioactive (R) materials out of regulatory control (MORC). The management of threats is the basis of the architecture design which addresses legal, organisational, operational, regulatory, and technical aspects of nuclear security. The architecture includes mobile detection capabilities and portal monitors reporting via reachback services. Under the leadership of the law enforcement, special CBRNE teams are formed with expertise from different competent authorities. Special emphasis should be placed on the fast resolving of alarms generated by the detection instruments.

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, law enforcement has the leadership. Technical reachback assists operations centres for alarm adjudication, or gives direct feedback to the frontline officers.

Technical reachback capacity mainly consists of analysing gamma spectra and neutron counts giving advice on nuclear security and radiation safety, as well as collecting and analysing complementary incoming information (pictures etc.). The experts performing analyses are located away from the field, where they are able to process the data remotely. If needed, the reachback centre may request additional measurements from the first responders, while the first responders may ask for radiological advice or precisions about the handheld detectors/spectrometers.

Coupled to information received from other sources, a decision is taken about the threat level, with the aim of discriminating between a real RN threat and a radiological problem. If a threat is confirmed, the national response plan is activated and law enforcement takes the leadership.

Reachback implementation varies in different countries. A basic service is a centre providing timely advice for the frontline officers regarding risks of RN materials. A more comprehensive implementation is a duty officer on call or a full 24/7 centre with comprehensive analysis capability. On the other hand reachback could also contain automated analysis services and related alarm generation. For more information on national reachback capabilities, see ERNCIP document [ERN 2015]

4. Data formats and protocols for cooperation

NSDAs, based on a holistic approach, define formats and protocols for data and information exchange between different technical and non-technical systems, including reachback and operational users. The first initiative to develop European formats and protocols was introduced in 2004 for airborne gamma spectrometry [TOI, 2004]. The principles presented in this publication are valid today, and the scope is more general, not limited to one detection technology.

In the past, the data formats did not contain metadata. Typically only the parameter values were given in a fixed format, defined character by character (Fortran records, for example). A clear improvement was made in 1996 in the gamma spectrometry data format of the Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO): the format contained tags which allowed adding different types of information, and in a different order. The format has served well for its original purpose, but has also caused trouble because there was no means to check the validity of the messages. Also, applying this format to other applications turned out to be problematic. The specification was not clear enough for expansions.

A sustainable data format is based on an international standard which provides a reliable means to describe the contents. The messages must contain enough information about the data itself. Besides a well-defined data format, an agreed protocol is necessary for efficient information management.

4.1. XML

Extensible Markup Language (XML) defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. XML is a standard maintained by the World Wide Web Consortium (W3C) ([8]). XML is an independent tool for carrying information, regardless of software and hardware.

XML is a textual data format and emphasises simplicity and usability. XML is used for the representation of arbitrary data structures and therefore it suits nuclear security well. The following example explains the basic idea:

```
<ERNCIP>
        <question>
                What needs to be done for the European
                critical infrastructure protection?
        </question>
        <answer>
                Develop a list-mode data acquisition standard and
                a data management standard for reachback services.
        </answer>
        <!—More questions and answers, please. —>
</ERNCIP>
```

([8]) World Wide Web Consortium, http://www.w3.org/

The data are placed between the tags defined by the users. Here there are three tags: ERNCIP, question and answer.

XML provides several advantages for data management.

- Text based — readable without special software; in an emergency, no special software is needed to get the key data; text files pass servers that scan for viruses.
- Extensible — to cover unforeseen applications; retains backward and forward compatibility.
- Validated — XML files can be checked ('validated') by machines for correct syntax.
- Resistance to data corruption — partial corruption does not destroy the whole message.

4.2. ANSI and IEC standards

There are two standards that are intended to define the data format produced by radiation detection instruments ([9]).

- IEC 62755 radiation protection instrumentation — data format for radiation instruments used in the detection of illicit trafficking of radioactive materials.

- ANSI/IEEE N42.42 — data format for radiation detectors used for homeland security.

IEC 62755 [IEC, 2012] was adopted from ANSI/IEEE N42.42 [ANS, 2006]; therefore, their contents are the same. The purpose of the standard data format is to facilitate manufacturer-independent transfer of data and information from radiation measurement instruments to the analysis resources which could be located on-site or far away in a reachback centre. An application domain of the standards is nuclear security, especially the detection of illicit trafficking of MORC.

The original ANSI/IEEE N42.42 standard was developed to address the need to have a common data format to analyse the data provided by different types of radiation detection systems (personal radiation detector (PRD), spectroscopy-based radiation portal monitor (SPRD), radionuclide identification detector (RID), radiation portal monitor (RPM), spectroscopy-based radiation portal monitor (SRPM), backpack radiation detector (BRD) mobile systems). The design basis of the standard was XML which provides a format that is vendor-neutral.

These standards consider radiation measurement systems that have several types of components (e.g., video, occupancy sensors). The radiation detectors are the primary components. They generate the raw measurement data in response to a radiation field. Radiation measurements are sequentially recorded and metadata (e.g., photos, specific type of data, bar scans, notes) can be easily incorporated into the XML file.

A specific validation tool was created by the ANSI/IEEE N42.42 standard working group to help instrument testers and vendors check for the validity of the XML files ([10]). This tool applies for both the IEC and the ANSI/IEEE standards, as they have identical format requirements.

An example of an ANSI 42.42 data file can be found in Appendix 3.

([9]) IEC 62755 schema http://www.nist.gov/pml/div682/grp04/iecn42.cfm
ANSI 42.42 schema http://www.nist.gov/pml/div682/grp04/upload/n42.xsd

([10]) Validation tool https://secwww.jhuapl.edu/n42/Account/LogOn

4.3. Linssi format

Linssi is a structured query language (SQL) database for gamma-ray spectrometry. It is being developed in collaboration with STUK, the Aalto University, and the Radiation Protection Bureau, Health Canada (HC). Linssi is freely available for all registered users. Full documentation of the database, including scripts to create the database and several scripts to use it, are available at Aalto University [AAR, 2008, 2011]. Linssi development started in 2002 in Finland and its first version was online in 2003. Full documentation, including the database, schema and related scripts [ALA, 2011], has been available since 2006. The latest version 2.3 of Linssi was released in August 2011.

The Linssi database creates a solid foundation for the communication of data and analysis results. The system defines the data storage protocol. All input-output (I/O) processes have to obey the rules of the database, including acknowledgement of certain reserved words.

For rigorous data exchange, an XML data format was defined that follows precisely the structure of the Linssi database. This approach guarantees maximum interplay between the data format and the database which also serves as an interface between different automated and interactive processes. The Linssi data file has an extension of LML. It refers to Linssi markup language which follows strictly the XML standard, including schema definition. In addition, software tools are made freely available for creation of the Linssi database (maketables), and for data and information upload (lmltodb) and download (dbtolml). The Linssi database and its tools allow building an efficient data management system for nuclear safety and security, including in-field measurement and laboratory analyses. No other system is available from open-source domain.

The Linssi data structures suit particularly well for reachback services because they support one object to be measured several times and analysed several times (Figure 1). An example LML data file is in Appendix 4, and the data analysis principle is described in Appendix 5.

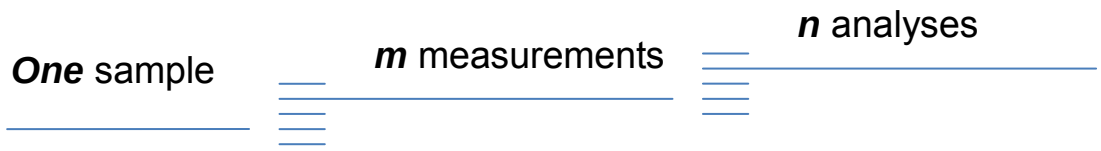


Figure 1. Basic data structures of Linssi. A sample can be measured ***m*** times and any spectrum can be analysed ***n*** times. Auto increment keys of the database engine keep track on the operations. This data structure makes it very easy to retrieve data from the database. For example, knowing the sample identification key makes it possible to find all measurement and analyses related to it, and vice versa, knowing the analysis identification key gives immediately the pointer to the sample and to all measurement data.

4.4. Data exchange protocols

A data exchange protocol defines the syntax and mechanisms for communication. NSDA is so complex that an agreed data handling protocol is a critical requirement for cooperation between competent authorities, particularly for automated processes consisting of data, analyses, alarm messages and auxiliary information.

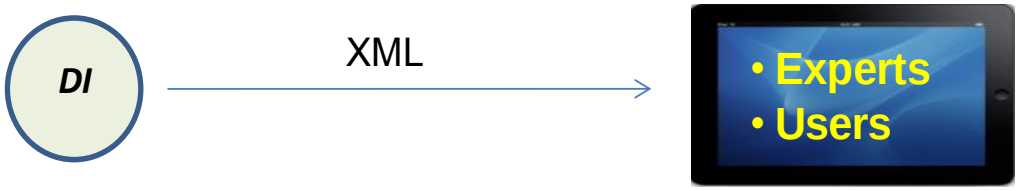
A data handling protocol should be developed into a technical standard ([11]). This may be a non-trivial effort. In nuclear security no such protocol has been defined at the international level. However, the open-source database Linssi is used as a data storage in many institutions, for example in Finland (STUK), France (ISRN), Canada (HC), Germany (BfS) and Ukraine (SSTC NRS). Linssi defines implicitly a protocol for the users to handle the data, information and knowledge created in various phases of the detection and alarm adjudication processes (Figure 2). All users talk to the database, not to each other.

The advantages of a data handling protocol, based on a standard database, are as follows.

- Efficient interoperability becomes possible between competent authorities and Member States.
- Data and information provided by the instrument grows to knowledge through expert analysis (via reachback).
- The changes needed to be made in existing data acquisition systems are minimal.
- Remote analysis capability may change the way the instruments operate in the future. Instead of local analysis, the data are processed at a remote server and the results are returned in real time via cell phone, e-mail or web page.
- A rapid response can be achieved with less man power.

([11]) The smart sensor interface standards may be applicable here: IEEE 1451 and ISO/IEC/IEEE 21451.

(a)



(b)

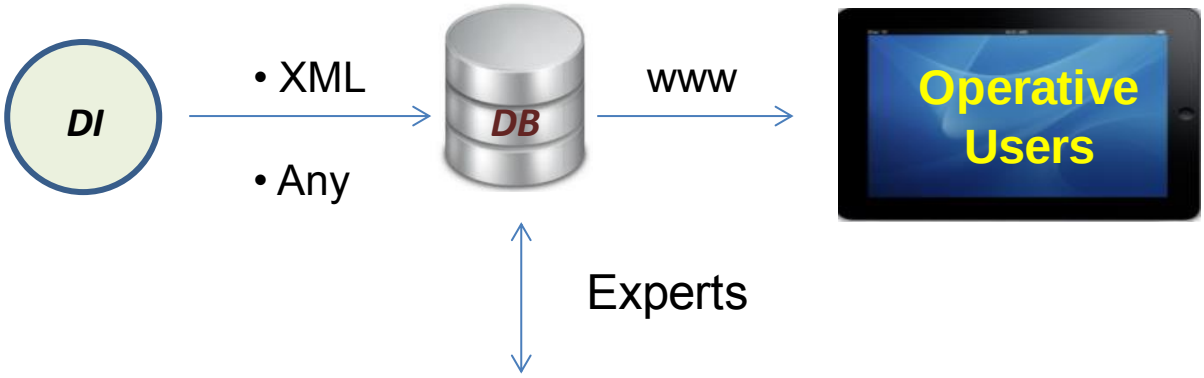


Figure 2. Communication between the detection instruments (DI) and the users. (a) The system has a well-defined XML format but no protocol to handle the contents (present status). (b) The lower system is also based on a fixed XML format but it can also accept other application-specific data (present Linssi architecture). The common interface is the database (DB) which actually defines the protocol because the detection instruments and the users must obey its data structures. Format 'Any' refers to specific application which writes directly to the database; i.e., the application software uses tools of the database engine to upload measurement data directly. Today, DI and DB can be physically distant and they could be connected via a virtual private network (VPN), as if they were in physical connection.

5. Discussion and conclusions

Strengthening CBRNE security in the European Union reduces the threat of and damage from CBRNE incidents [EC, 2009, 2010]. However, there are 'good reasons to believe that the threat from CBRN materials and explosives remains high and is evolving' [EC, 2012]; therefore, EU will 'further support CBRN-E research, testing and validation activities, and progress towards appropriate detection standards adapted to each type of environment, including projects such as ERNCIP' [EC, 2014].

One of the main issues facing the EU security industry is its highly fragmented nature, exhibiting a lack of standardisation and harmonised certification procedures. The need for standardisation of information sharing between competent authorities and international bodies regarding radiation measurements and data analyses has been recognised by CEN/TC 391, which executes the European Commission Mandate M/487 to establish European security standards.

The RN thematic group of ERNCIP has made an initiative to develop an IEC standard for list-mode digital data format for nuclear instrumentation [KEI 2014]. Similarly, as explained in this report, there is a need to improve standardisation at the data management level. For data formats there exists ANSI/IEEE and IEC standards but there is no agreed protocol for data management, information sharing and analysis. Not only standard formats but also standard protocols are necessary for the success of reachback services.

The RN thematic group has identified a need to standardise the protocol for reachback and for other domains of nuclear data sharing. The protocol could be built around common database structures.

Not all EU Member States do have the capabilities to process data provided by nuclear security instruments. Therefore the Member States should consider having coordinated capability available for a more efficient and comprehensive approach to responding to future nuclear threats. This could be achieved by a few reachback centres in Europe. These centres would be built upon existing national facilities and expertise and would provide analysis services for alarm adjudication and other security needs. This would be enabled by data and information sharing across the Member States. Efficient data processing is only possible if standard protocols are agreed.

The United States provides reachback services for those who want to send their data for processing. The United States' approach is based on standardisation of formats or some conversion software is used between different formats. This is labour-intensive. Stricter requirements should be put on protocols. Once this is agreed, an efficient technological solution can be achieved for reachback services.

The RN thematic group proposes that a European or an international standard for a data storage protocol on nuclear and radiological data exchange be developed, using a common database as the basis (see Figure 3). The starting point of the work could be the open-source database Linssi. In addition, the new system should be designed to incorporate list-mode data. Work on further developing these ideas will be carried out by the ERNCIP RN thematic group during 2015, aiming at proposals for harmonisation/standardisation of information sharing to enable remote expert support for field teams.

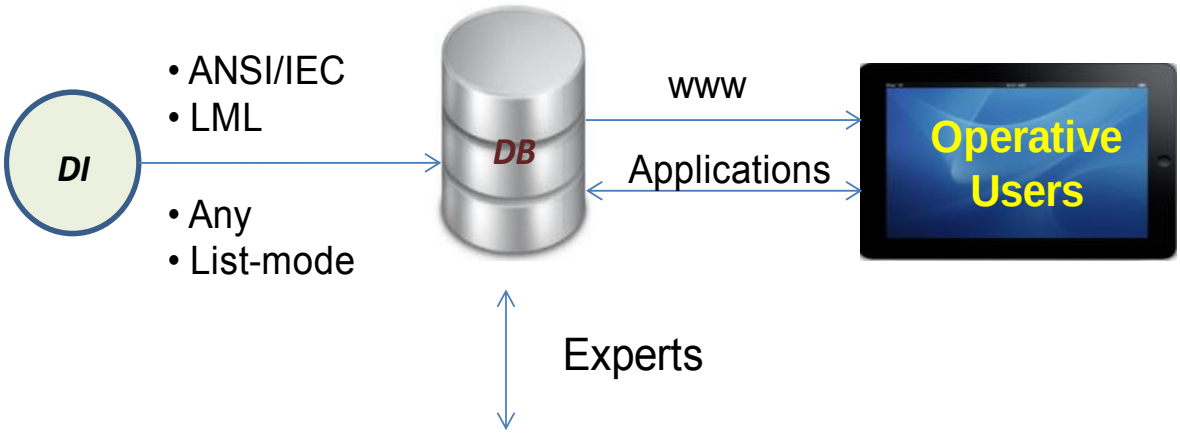


Figure 3. Future comprehensive data management system for reachback. It contains standard formats (XML) and a protocol which is a database defining precisely how the data must be uploaded or retrieved. All users interact with the database, not with each other. The integration of list-mode data is new element, as compared with Figure 2b.

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), pp. 631–637.

[AAR 2011] Aarnio, P., Ala-Heikkilä, J., Hoffma,n 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

[ACK, 1989] Ackoff, R. L. 'From data to wisdom', *Journal of Applied Systems Analysis* 15: pp. 3-9.

[ALA 2011] Ala-Heikkilä, J., Aarnio, P., 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 II: script and interfaces, Version 2.3' *Helsinki University of Technology Publications in Engineering Physics Report*, TKK-FA861 (2011). Available at http://linssi.hut.fi/scripts_23.pdf.

[ANS, 2006] ANSI/IEEE N42.42. Data format for radiation detectors used for homeland security, 2006.

[BUC, 2009] Buckley, W. and Allen, R., 'The importance of technical reachback in the adjudication of radiation alarms', *LLNL-CONF-411428, IAEA International Symposium on Nuclear Security*, Vienna, Austria, 2009.

[DIC, 2010] *Dictionary of military and associated terms*, United States Department of Defense 2010.

[EC, 2009] 'European Commission, Communication from the Commission to the European Parliament and the Council on strengthening chemical, biological, radiological and nuclear security in the European Union — an EU CBRN action plan', COM(2009) 273 final, Brussels, 2009.

[EC, 2010] 'European Commission, Communication from the Commission to the European Parliament and the Council. The EU internal security strategy in action: five steps towards a more secure Europe', COM(2010) 673 final, Brussels, 2010.

[EC, 2012] 'European Commission, 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', COM(2012) 0417 final., Brussels, 2012.

[EC, 2014] 'European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks', COM(2014) 247 final, Brussels, 2014.

[GIC, 2009] *Global initiative to combat nuclear terrorism. GICNT, model guidelines document for nuclear detection architecture* 2009, vol I.

[HOR, 2014] Horizon 2020, European Commission, 'Work Programme 2014 — 2015; 14. Secure societies. Protecting freedom and security of Europe and its citizens: Fight against crime and terrorism'. H2020-FCT-2015. (Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials.)

[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.

[IEC, 2012] IEC 62755. 'Radiation protection instrumentation — data format for radiation instruments used in the detection of illicit trafficking of radioactive materials', 2012.

[KEI, 2014] Keightley J., Paepen, J., Tengblad, O., Toivonen, H. and Peräjärvi, K. 'List-mode data acquisition based on digital electronics.', *EUR 26715, ERNCIP 2014. Report JRC90741*. Luxembourg 2014.

[NAT, 2010] NATO/PfP, 'Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear Incidents.', *ATP-45(D), Operators Manual*, 2010.

[PAE 2014] 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.', Report *JRC93260, EUR 26976*, Luxembourg 2014.

[TOI, 2004]Toivonen, H., 'Airborne gamma spectrometry — towards integration of European operational capability.', *Radiation protection dosimetry (2004)*, Vol. 109, pp. 137–40.

Appendix 1: categorisation of terms for communication

Definitions adopted from Wikipedia:

1. **Raw data** is unprocessed data; it refers to a collection of numbers and characters.

2. **Data** is a set of values of qualitative or quantitative variables. Data in data processing is represented in a structure that is often tabular, a tree, or a graph. Data is typically the result of measurements and can be visualised using graphs or images ([12]).

3. **Information** is what informs. Information is conveyed either as the content of a message or through direct or indirect observation of something. What is perceived can be construed as a message in its own right, and in that sense, information is always conveyed as the content of a message. Information can be encoded into various forms for transmission and interpretation ([13]).

4. **Knowledge** is a familiarity, awareness or understanding of something, such as facts, information, descriptions, or skills, acquired through experience or education by perceiving, discovering, or learning ([14]).

5. **Wisdom** is the ability to act using knowledge, experience, understanding, common sense, and insight. Wisdom is a habit or disposition to perform the action with the highest degree of adequacy under any given circumstance. This implies a possession of knowledge or the seeking thereof in order to apply it to the given circumstance ([15]).

([12]) http://en.wikipedia.org/wiki/Data
([13]) http://en.wikipedia.org/wiki/Information
([14]) http://en.wikipedia.org/wiki/Knowledge
([15]) http://en.wikipedia.org/wiki/Wisdom

Appendix 2: ROOT framework for list-mode data processing in particle physics

ROOT([16]) is a framework for data processing, born at CERN. Every day, thousands of physicists around the world use ROOT applications to analyse data or to perform simulations.

- **Save data.** The data is saved in a compressed binary form in a ROOT file. The object format is saved in the same file. ROOT provides a data structure that is extremely powerful for fast access of huge amounts of data — orders of magnitude faster than any database.
- **Access data.** Data saved into one or several ROOT files can be accessed from PC, from the web and from large-scale file delivery systems used e.g. in **the WLGC**. ROOT trees spread over several files can be chained and accessed as a unique object, allowing for loops over huge amounts of data.
- **Process data.** Powerful mathematical and statistical tools are provided to operate the data. The full power of a C++ application and of parallel processing is available. Data can also be generated following any statistical distribution, making it possible to simulate complex systems.
- **Show results.** Results are best shown in histograms, scatter plots, fitting functions, etc. High-quality plots can be saved in PDF or other format.
- **Interactive or built application.** One can use the CINT C++ interpreter or Python for interactive sessions and to write macros, or use compiled programs to run at full speed. In both cases, one can create a graphical user interface.

([16]) http://root.cern.ch/drupal/

Appendix 3: example ANSI 42.42 data file

This example is very simple, containing only a spectrum and its energy calibration [ANS, 2006]. There is some optional information in this example: all the time information (<StartTime>, <LiveTime>, and <RealTime> elements) and the energy calibration (the <Calibration> element and everything in it) could be omitted if the data was not available or required. Note that the leading <? xml?> element and namespace information is not present. These items are strongly recommended but are not absolutely required; the file cannot be validated without this information.

```
<N42InstrumentData>
<Measurement>
        <Spectrum>
                <StartTime>2003-10-22T23:45:19</StartTime>
                <RealTime>PT60S</RealTime>
                <LiveTime>PT59.61S</LiveTime>
                <Calibration Type="Energy">
                        <Equation Model="Polynomial">
                                <Coefficients>-10 2.99</Coefficients>
                        </Equation>
                </Calibration>
                <ChannelData>

                        0 0 0 0 0 0 0 0 0 0 0 0 3 9 5 12 4 6 5 4 3 4 3 3
                        ....
                        0 2 1 1 0 1 1 0 0 2 1 1 0 1 1 0
                </ChannelData>
        </Spectrum>

</Measurement>
</N42InstrumentData>
```

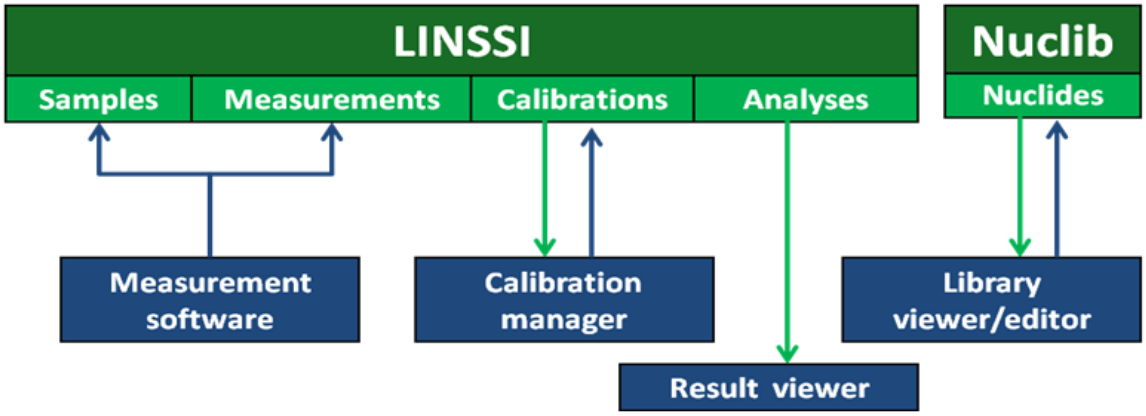
Appendix 4: example Linssi data file, (*.LML)

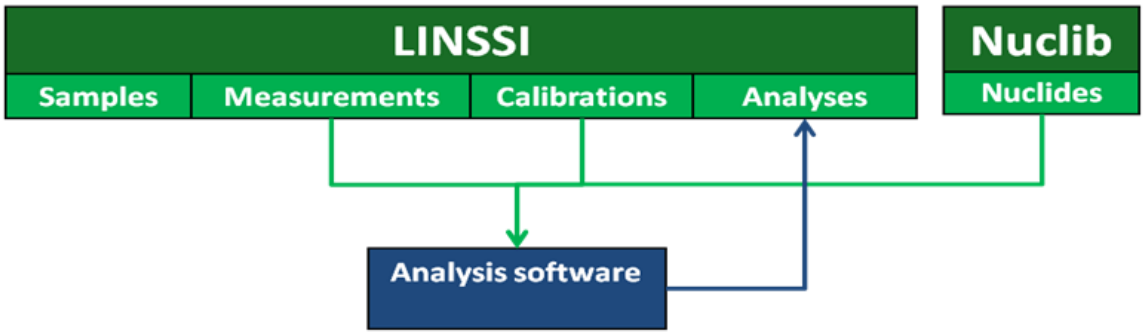
This example describes the first part of an LML file containing data related to a sample and to its measurement. The example does not contain analysis results. In addition, a complete LML file is more complex containing other information, such as <calibrationData> and <generalData> data blocks which specify calibrations, either data pairs or coefficients of calibration functions (energy, resolution, efficiency) and administrative information, for example detector code and measurement setup. The file structure supports add-on tables, such as details related to alarms <alarms>.

<?xml version="1.0' encoding="iso-8859-1'?>
<LML xmlns="http://www.stuk.fi/Linssi">
<sampleData>
<samples>
<sampleId>Thule</sampleId>
<facilityId>STUK-TTL</facilityId>
<sampleType>particle</sampleType>
</samples>
<**measurementData**>
<measurements>
<measId>NaI3x3_01_2008-10-14_16:55:00</measId>
<acqStart>2008-10-14 16:55:00</acqStart>
<acqEnd>2008-10-29 09:35:00</acqEnd>
<acqRealTime>1188902</acqRealTime>
<acqLiveTime>1177013</acqLiveTime>
<measSetupId>NaI3x3-001</measSetupId>
<measurementType>NaI3x3</measurementType>
</measurements>
<spectra>
<firstChannel>0</firstChannel>
<lastChannel>4095</lastChannel>
<idSpectrum>000</idSpectrum>
<spectrumType>meas-NaI3x3</spectrumType>
<spectrum>
0 23 11 52
…..
0 112
</spectrum>
</spectra>
</measurementData>
</sampleData>
<generalData>
…

Appendix 5: Linssi database and data processing principles around the database

After data upload to Linssi database, each software component performs a small piece of work from a larger system taking its input from the database and then writing its results back to the database. All modules communicate with the database, not with each other. This architecture makes it easy to improve any piece of the system because it has minimum impact on what the other modules are doing. NUCLIB database is outside Linssi but it is still closely integrated to Linssi's data structures. NUCLIB database is a comprehensive nuclide library based on evaluate nuclear structure data file (ENSDF) ([17]).





([17]) ENSDF library. http://ie.lbl.gov/databases/ensdf-manual.pdf

European Commission
EUR 27099 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Remote Expert Support of Field Teams - Reachback Services for Nuclear Security.

Authors: Harri Toivonen, STUK — Finland
Per Reppenhagen Grim, DEMA — Denmark
Olof Tengblad, CISC — Spain
John Keightley, NPL — United Kingdom
Jan Paepen, European Commission
Kamel Abbas, European Commission
Frank Schneider, Fraunhofer Institute — Germany
Jonas Nilsson, Lund University — Sweden
Kari Peräjärvi, STUK — Finland

2014 – 34pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-45418-9

doi:10.2788/20613

Abstract

Strengthening chemical, biological, radiological, nuclear and explosive (CBRNE) security in the European Union (EU) reduces the threat of and damage from CBRNE incidents. One of the main issues facing the EU security industry is its highly fragmented nature, exhibiting a lack of standardisation and of harmonised certification procedures. The need for standardised information sharing between competent authorities and international bodies regarding radiation measurements and data analysis has been recognised by several experts in response to Commission mandate M/487 for the establishment of European security standards. This report will suggest a way forward to develop protocols for more efficient cooperation between competent authorities and remote expert support or reachback centres at the national and international level. Not all EU Member States have the capabilities to process data provided by nuclear security instruments, and thus should consider instigating a coordinated capability yielding a more efficient and comprehensive approach in responding to future nuclear emergencies. This could be achieved by reachback centres across Europe (built upon existing national facilities and expertise) and would provide analysis services for alarm adjudication. Efficient data sharing and processing across EU Member States requires the use of standard data formats and protocols.

LB-NA-27099-EN-N

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.

doi:10.2788/20613

ISBN 978-92-79-45418-9