
Harri Toivonen
HT Nuclear Ltd, Finland

Magic Maggiore, Technical Reachback Workshop, EC/JRC/ERNCIP and GICNT ISPRA, 28-30 MAR 2017

This work has received funding from the European Union’s Horizon 2020 research and innovation programme. The European Commission’s support is gratefully acknowledged.

The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Commission.
Solutions are needed to detect nuclear threats to critical infrastructure and to mitigate consequences.

Topics being analysed by this network of experts are:

1) List-mode data acquisition based on digital electronics
2) Robotics - radiation detection with unmanned systems
3) Reachback - expert support to field teams.

https://erncip-project.jrc.ec.europa.eu/
Contents

1. Expert Support in Nuclear Security
2. Role of Information
3. Law Enforcement Needs and Expert Support
4. Reachback Technology
5. Conclusions
Nuclear Security Activities

- Detection architecture includes:
  - Threat assessment
  - Detection
  - Assessment of the alarms and alerts

Nuclear experts have a crucial role on many areas of nuclear security, such as planning of the architecture, and detection and analysis measures.
Geographic Layers of NSDA
Global View to Pathways

1. Designated POE
   - Customs

2. Undesignated POE
   - See coast
   - Green Border

3. MPE

A. Exterior

B. Border

C. Interior

- Frontier Guard
- Expert organizations
- Regulatory body
- Nuclear facilities, industry, hospitals, laboratories

Target

Safe and secure society

Rescue
Transport authorities
Police

Detection of MORC Material Out of Regulatory Control

National priorities based on IAEA/GICNT documents

Framework

Capabilities

Areas of interest
Instrument deployment
Expert support (*)

(*) Cross-cutting element

Nuclear Security Detection Architecture

Exterior
Facilities
Transport
Border

Border
Int. transport
Border
Facilities

Interior
Transport
Stand-off
Target
Expert Support

- Expert support is a process that brings remote resources to the field teams (law enforcement, customs, ..)
- The support is of vital importance for the assessment of the in-field measurements and adjudication of alarms.
- A well-designed programme of expert support separates the measurement and analysis processes.

Expert support can be provided by

1. Specialist team arriving to the site
2. Remotely (information sharing, analysis, advice)
Reachback = Expert Support

- In a radiological emergency, **data analysis** plays a key role in providing a factual basis for deciding on the counter measures.

- Reachback technology must be knowledge-driven: i.e. must produce knowledge and wisdom ("**what to do next**") for the operative units, rather than data and unverified analysis results.

- A State may allocate this task to an agency, such as the Radiation Safety Authority. The operational unit is called as **Reachback Centre**.
Command and Control (CC)

Operations Centre

Operative information

Expert Support
Scientific and technical information

Operative units

1,2,3
4,5
1,2,3
# Expert Support
## Different Reachback Services

<table>
<thead>
<tr>
<th>Level</th>
<th>Organization</th>
<th>Functionality - Role</th>
</tr>
</thead>
</table>
| **A**  | **Subject Matter Experts (SME)** | POC - Point of Contact  
Call Centre  
Advice to Law Enforcement |
| **AA** | **Expert Support Centre**  
(Reachback Centre) | *As above*  
**Technical Support**  
- Detection systems: implement, maintain, sustain, QC  
- Training, exercises  
- Mobile teams with basic capability  
**Scientific Support**  
Analysis support on request  
Alarm assessment and support to adjudication |
| **AAA** | **Advanced Expert Support Centre**  
(Advanced Reachback Centre) | *As above*  
**Operational Support**  
- Integrated to operative units  
- CBRNE teams, Render safe, Crime scene management,..  
**Advanced Technical and Scientific Support**  
- Operation of large real-time detection networks  
- Advanced analysis support 24/7  
- Material characterization  
- Alarm adjudication |
Contents

1. Expert Support in Nuclear Security
2. Role of Information
3. Law Enforcement Needs and Expert Support
4. Reachback Technology
5. Conclusions
Role of Information in the Detection Architecture

Technical and non-technical information is generated from many sources:

- Identification of suspicious activities
- Detection, identification and localization (MORC)
- Characterization of material
- Evaluation of effectiveness of the detection systems
- Production of situational awareness
## Types of Information

<table>
<thead>
<tr>
<th>Threat and Alarm or Alert Information</th>
<th>Configuration Information</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential or actual nuclear security event</td>
<td>Setup and organization of detection assets</td>
<td>State of health</td>
</tr>
<tr>
<td>Requires timely delivery to users</td>
<td>Assists operation managers and technical support</td>
<td>Enables a rapid and effective response</td>
</tr>
</tbody>
</table>

Type of information varies and different competent authorities have different needs.
Categorization of Terms for RN Measurements and Related Information Products

1. **Raw data**
   - Time-stamped events detected by instruments

2. **Data**
   - Spectra generated from raw data at certain intervals

3. **Information**
   - Messages in compact format (metadata, data, raw data, initial analysis results)

4. **Knowledge**
   - Verified information consisting of nuclide identification, activity estimation, …

5. **Wisdom**
   - Appropriate decision-making based on the attained knowledge. A message which is useful for the frontline officers to interdict.
Alarm Adjudication
Cooperation between Competent Authorities

Procedures and protocols must be in place for a prompt determination of potential threat

Alarm or alert

Alarm Adjudication

Initial Assessment

Assessment process

Determine the outcome in a timely manner
Competent Authorities for Prevention, Detection, and Response

How a competent authority knows what is relevant information for another organization?
Contents

1. Expert Support in Nuclear Security
2. Role of Information
3. Law Enforcement Needs and Expert Support
4. Reachback Technology
5. Conclusions
Law Enforcement Needs for Expert Services
Cooperation between Competent Authorities

1. Experts support 24/7 field operations (planning, analysis, advice, safety, ...)

2. Experts give operational support to Command and Control in a Nuclear Security Event (NSE) or potential NSE

3. Experts are part of the field operations (advanced measurements, advice, safety, ...)

4. Regulatory body is the primary operator; law enforcement supports (render safe, transport, ...)
Operations Centre

• Has the leadership in response actions

• Maintains situational awareness

• Contributes to the adjudication of alarms and alerts

• Directs resources and assets in response to alarms and alerts

• Facilitates coordination and communication among local, national, and international entities
Nuclear Experts for Security

RN scientists or inspectors have relevant expertise on

- Nuclear and other radioactive materials
- Implementation of detection systems
- Laboratory measurements and analyses
- Analysis of data from detection instruments
- Reachback resources
- Scenarios, consequences (risk-informed approach)

Where the subject matter experts come from

- Nuclear Regulatory Authority
- National Laboratories
- Academic Organizations
- Technical Support Organizations
- Industry
Tasks for Expert Support

Operational

Advice to law enforcement
Advanced measurements
Initiation of response protocol (together with CC)
Threat object neutralization - render safe, source recovery
Safety assessment – consequence analysis

Scientific

Analysis of measurement data
Alarm adjudication - nuclear security event?
Material characterisation - nuclear forensics

Technical

Instrument deployment
Quality control of data
State-of-health of detection systems
Network management
Education
Training and exercises
## Tasks for RN Field Operations

<table>
<thead>
<tr>
<th>Item</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Spectrum acquisition</td>
</tr>
<tr>
<td>Identification</td>
<td>False/Innocent/True Alarm</td>
</tr>
<tr>
<td>Localization</td>
<td>Human knowledge</td>
</tr>
<tr>
<td>Source characterisation</td>
<td>Scientific expertise</td>
</tr>
<tr>
<td>Risk estimation</td>
<td>Safety and Security</td>
</tr>
<tr>
<td>• Activity</td>
<td>• Automated</td>
</tr>
<tr>
<td>• Shield properties</td>
<td>• Difficult in unknown geometry</td>
</tr>
<tr>
<td>• Threat reduction</td>
<td>• Not performed by FLO</td>
</tr>
<tr>
<td>• Mitigation, resilience</td>
<td>• Simple safety rules</td>
</tr>
<tr>
<td>• Mitigation, resilience</td>
<td>• Countermeasures?</td>
</tr>
</tbody>
</table>
## Tasks for RN field measurements

<table>
<thead>
<tr>
<th>Item</th>
<th>Way forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td><strong>List-mode; Robotics; Reachback</strong></td>
</tr>
<tr>
<td></td>
<td>• CBRNE Sensor arrays</td>
</tr>
<tr>
<td></td>
<td>• Time frame is an analysis issue</td>
</tr>
<tr>
<td>Identification</td>
<td><strong>Analysis improvements</strong></td>
</tr>
<tr>
<td></td>
<td>• Embedded in local system</td>
</tr>
<tr>
<td></td>
<td>• Cloud services (reachback)</td>
</tr>
<tr>
<td>Localization</td>
<td><strong>Novel technologies</strong></td>
</tr>
<tr>
<td></td>
<td>• Operative use very soon</td>
</tr>
<tr>
<td></td>
<td>• Different technologies</td>
</tr>
<tr>
<td>Source characterisation</td>
<td><strong>Novel analysis methods</strong></td>
</tr>
<tr>
<td>• Activity</td>
<td>• Possible when source localization issue is solved</td>
</tr>
<tr>
<td>• Shield properties</td>
<td></td>
</tr>
<tr>
<td>Risk estimation</td>
<td><strong>Well-justified response</strong></td>
</tr>
<tr>
<td>• Threat reduction</td>
<td>• Source characteristics available</td>
</tr>
<tr>
<td>• Mitigation, resilience</td>
<td></td>
</tr>
</tbody>
</table>
Contents

1. Expert Support in Nuclear Security
2. Role of Information
3. Law Enforcement Needs and Expert Support
4. Reachback Technology
5. Conclusions
From Detectors to Reachback

- Human operators (FLO)
- Advanced detection systems
- Robotics for field

**Administrative measures**

- Information sharing
- Resources sharing
- Cooperation
  - nationally
  - internationally
  - bilaterally

**Standards for data structures**

- Fast and reliable communication

**New secure IT solutions for data transfer**

- Advanced data handling
  - Standard database and software
  - Reachback Centres
Spectra and other data are transferred to a remote data server for reachback → situational awareness
Fast and robust data transfer:
1. Prioritization of alarms
2. Recovery from breaks (no data lost)
3. Large amount of data
   - Clever data transfer algorithm (adapt to bandwidth, zip)
4. Encryption
Reachback Technology

Standard formats and protocols for information sharing

Finnish LINSSI
- Use common interfaces for data exchange
- Upload data to a shared data server
- Give services to all relevant partners

NATO MAJIIC

US NIEM

The users exchange data through the server, not directly with each other

ERNCIP Recommendation

XML → DB → www
Experts

Operative
Users
Contents

1. Expert Support in Nuclear Security
2. Role of Information
3. Law Enforcement Needs and Expert Support
4. Reachback Technology
5. Conclusions
Need for Novel Technologies

• **Timeliness**
  – Authorities must counter the adversaries in a rapidly changing environment
  – Detect, analyze, communicate and act

• **Detection sensitivity**
  – New type of sensors and data acquisition systems
  – Building detection arrays

• **Different needs by different users**

• **Cooperation**
  – National
  – International or bilateral

• **Massive data flow**

• **Lack of international standards**
Lack of Awareness of authorities is the main inhibitor to implement Reachback

• **Blindness to the risk**
  – It won’t happen in my country!
  – Why doing it now?
  – We are a nuclear-free zone!

• **Where the responsibility lies**
  – Somebody else takes care of this!

• **Fear of the costs**
  – Other threats and risks are more important!

• **Need for reachback technology**
  – Not understanding the benefits
  – Not talking the same language (reachback terms to glossary, CEN/TC391 WG2 CBRNE)
Joint Protocols

States should develop joint data structures, databases and software for efficient cooperation in nuclear security.

See the ERNCIP web page for the published reports (*):

- Remote expert support of field teams
- National reachback systems for nuclear security
- Information sharing in a nuclear security event

(*) The Reports:
https://erncip-project.jrc.ec.europa.eu/downloads
Novel in-field technologies provide **timely knowledge** through **reachback** to detect nuclear threats and to implement a balanced response.

\[ \int I(1, 2, 3) \ast RB \, dt = I(4, 5) \]

THE END

This work has received funding from the European Union’s Horizon 2020 research and innovation programme. The European Commission’s support is gratefully acknowledged. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Commission.