Managing the Security of Radioactive Sources

RON CAMERON, Australian Nuclear Science and Technology Organisation
PMB 1 Menai, NSW 2234

Summary : The issue of security of radioactive sources had arisen as a result of incidents where people were unintentionally exposed in various parts of the world. However after 11 September 2001, the focus on security was intensified by concerns over those who might wish to use radioactive sources for malevolent purposes. This paper will discuss the questions of the type and nature of these concerns and outline a process for assessing the threat and then assigning security measures for sources. This paper is based on work done by the author while at the IAEA and published as part of Tecdoc 1355.

1. INTRODUCTION

There are some millions of sources in use around the world delivering a wide range of benefits in medicine, industry and research. For example, there are estimated to be around 300 large industrial irradiators (from 0.37 to 370 PBq) and many more smaller irradiators. In the US alone, there are some 2 million industrial gauges. While these have many benefits they also pose a hazard if not properly controlled. The IAEA has published a number of reports that describe the human health consequences of unintended exposure to uncontrolled sources [1–5]. In addition to these considerations, the economic losses can be considerable. It has been reported that *"In total, the direct and indirect costs in Mexico for the remedial actions after the accident in 1983, when a teletherapy source was accidentally melted, is estimated to be about 34 million US dollars"* [6].

The International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (BSS) [7] specifically requires [para. 2.34] that:

> *"Sources shall be kept secure so as to prevent theft or damage and to prevent any unauthorized legal person from carrying out any of the actions specified in the General Obligations for practices of the Standards (see paras 2.7–2.9), by ensuring that:*
>
> *(a) control of a source not be relinquished without compliance with all relevant requirements specified in the registration or licence and without immediate communication to the Regulatory Authority, and when applicable to the relevant Sponsoring Organization, of information regarding any decontrolled, lost, stolen or missing source;*
>
> *(b) a source not be transferred unless the receiver possesses a valid authorization; and*
>
> *(c) a periodic inventory of movable sources be conducted at appropriate intervals to confirm that they are in their assigned locations and are secure."*

However, before 11 September 2001, the security of radioactive sources was largely addressed by measures protecting the sources from unintentional access by inappropriately qualified personnel or attempts at theft for financial gain. This assumption has now had to be modified to also include the need to prevent access to certain sources by people deliberately and malevolently seeking to cause radiation exposure or dispersal of radioactive materials. One known case of an attempt to malevolently use radioactive material occurred in 1995 when Chechens placed a container with ^{137}Cs in a Moscow park [8]. Fortunately, the material was not dispersed. In a news article [9] regarding a difference case, it was reported that *"six Lithuanian nationals were arrested in the Lithuanian capital, Vilnius, in a raid...during which a large amount of radioactive metal, ^{137}Cs, was confiscated."*

2. MOTIVATIONS FOR SECURITY

A number of serious incidents have occurred around the world because of orphan sources. The most significant was that in Goiania in Brazil [1] but other have occurred in Georgia in 1997 [3] and in Thailand in 1999 [5]. Many steps have been taken to address these concerns. Among these is the work by the IAEA in:

- conducting major conferences in Dijon (1998) and Buenos Aires (2000).
  development of an Action Plan and Revised Action Plan to improve regulatory control, categorise the hazard, establish international undertakings and provide education and training.
- Setting up a working group to develop a Code of Conduct on the Safety and Security of Radioactive Sources
  Developing a new warning sign for high activity sources.

September 11th caused a major rethink of these activities to consider:

- What are the threats from terrorism?
  Which are the most desirable sources?
  How can terrorists obtain such sources?
  What can be done to prevent this?

It is worthwhile putting the risk from radioactive sources in context. The figure below shows source impacts relative to other agents.

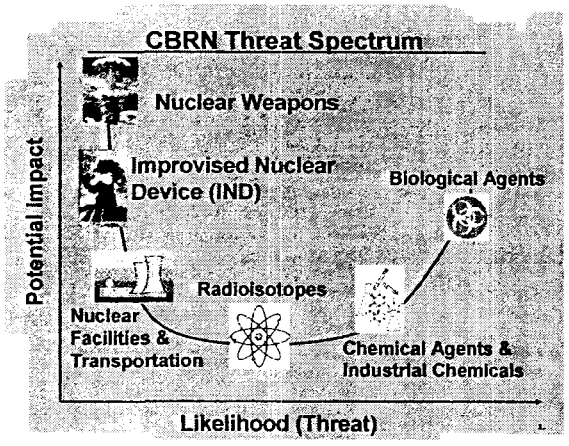

Figure 1 – WMD spectrum

This shows that the radiological threat has much less consequence than other agents, but it could still be a weapon of terror.

In tackling the security issue for sources, the relationship between safety and security is often debated. Source safety and security are intimately linked – many actions that enhance safety also enhance security and vica-versa. In addition, users need coordinated guidance in using sources and do not want to be confused by separate regulatory bodies and separate, and possibly conflicting, requirements.

The crucial question might seem to be "How do we made sources secure?", but this is too nebulous. We need, rather, a way of answering the question "How do we made sources secure enough?". That recognises the need for balance between allowing sources to be available for their beneficial purposes, while addressing the specific application appropriately. In addition that question allows us to consider the lifecycle, type and application of the source which will determine the requirements. The type of source varies greatly, from large radioisotopic thermoelectric generators to small moisture gauges, as shown in the Figures below.

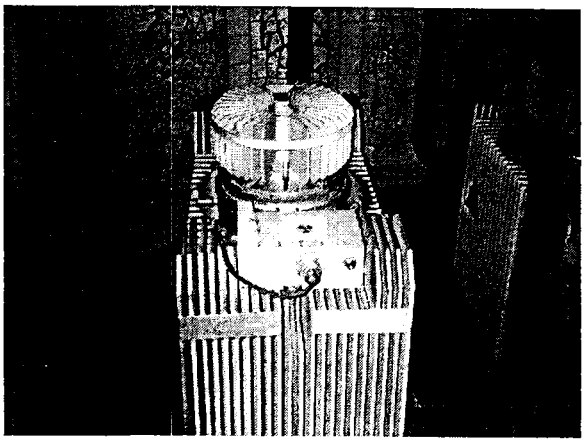

Figure 2 – Sr90 source with an activity of 40,000 Curies

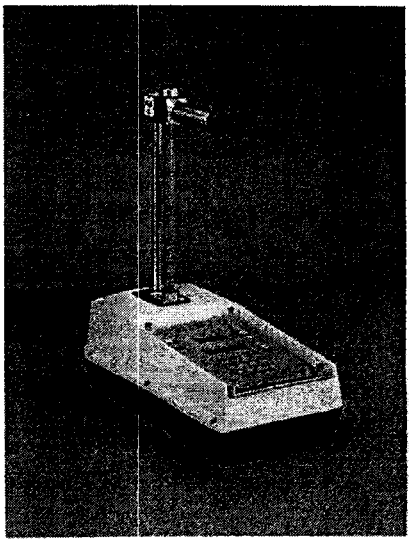

Figure 3 – Moisture density gauge

The question of security applies to the full range of sources, with significant activity and means that we need to ask:

> Is a hospital teletherapy source secure? Usually it is because the continual operation and the type of fixed container make removal difficult.
> Is an industrial radiography gauge secure? Probably much less so than a teletherapy

gauge, but then it contains much less activity.

- Is an orphan source secure? By its very definition, no, but there are other sources, while not yet orphaned, which are sufficiently vulnerable to be a concern.

3. GAINING CONTROL OVER SOURCES

There are two major aspects to ensuring control over sources. One is to have adequate licensing systems from manufacturer to disposal, so that the location and security of the source can be verified at all times. The Code of Conduct on Safety and Security of Sources [10] is an international undertaking that sets put principles for achieving this goal for higher category sources. It advocates import/export controls and national inventories, as well as enhanced regulatory requirements for security assessments. However this is just part of a general need to control sources at all points of their lifecycle including:

- Manufacture
- Supply
- Transport
- Use
- Storage
- Return to supplier
- Disposal.

Such a process requires international cooperation and cooperation between manufacturers, regulators and users.

The other aspect is to have remedial action programs that seek to identify and secure vulnerable and orphan sources worldwide. This is currently being done through the Tripartite Initiative for the Newly Independent States of the former Soviet Union. This is a joint IAEA/US/Russia program to locate and secure sources. However this needs to be globalised to other countries where sources may be vulnerable to unauthorised acquisition.

4. SECURITY DESIGN AND EVALUATION

There are several components of a complete overall security strategy:

(1) Appropriate manufacture and design of sources and devices to minimize the feasibility of malicious actions and maximize security.

(2) Management of sources only within an authorized, regulated, legal framework. Amongst other things, this includes efforts to:
   (a) provide a strong regulatory infrastructure;
   (b) prevent the unauthorized production of radioactive material;
   (c) validate legal purchases and ensure adequate justification for possession of sources;
   (d) ensure the reliability of personnel involved in managing sources.

(3) Prevention of acquisition of radioactive sources by those with malevolent intent. This includes measures to:
   (a) deter unauthorized access to the source, or source location, in order to deter theft;
   (b) detect any such attempts at unauthorized access;
   (c) delay unauthorized access or theft;
   (d) provide rapid response to attempts at unauthorized access or theft.

(4) Detection of actual theft or loss in order to appropriately respond and allow recovery efforts to start as soon as possible. This includes:
   (a) radiation, or other alarms;
   (b) accounting and inventorying.

(5) Efforts to recover any stolen or lost sources and bring them into secure regulatory control.

(6) Prevention of use for unauthorized purposes of any sources acquired improperly.

(7) Minimization of the accidental or malevolent consequences of any use.

This next section discusses ways to cover items 3 and 4.

4.1 Threat Assessment

The use of a design basis threat assessment methodology is recommended as the best method to design the security measures for specific sources. The design basis threat will vary quite widely according to the country, facility and source. Associated security measures should be commensurate with the threat and the level of risk acceptance. Threat assessments can range from being very detailed to quite generic. Security measures, likewise, can be very specific or based on generic assessments performed at an organizational or government level.

A detailed threat assessment provides the means of adjusting security provisions in accordance with the results of that analysis and more specifically addressing the potential consequences associated with loss of control over each specific source.

A detailed design basis threat assessment methodology to define the appropriate level of security consists of the following activities:

(1) Characterize the source, its type, nature and application (identify the target).

(2) Perform an assessment of the potential threat within the country as a whole, based on

information from security and intelligence experts.

(3) Evaluate the potential consequences of successful actions to acquire the source. This can range from theft with the intention to threaten action in order to cause panic, through to the deployment of a radiological dispersal device and the attendant consequences.

(4) Determine, based on the assessment of threat and potential consequences, a design basis threat against which the security should be designed and evaluated. For example, the threat may range from attempts by one person to gain access but without any special equipment through to a well-equipped and possibly armed group.

(5) Perform a vulnerability analysis for the specific source, or sources against this design basis threat.

(6) If there is a requirement to reduce the risk associated with unauthorized access and acquisition, then first optimize existing measures and then implement additional measures.

As noted, many of these measures may just be extensions or amplifications of the existing safety measures.

4.2 Security performance measures

Based on the vulnerability analysis for a specific source, an assessment of the risk can be made. The level of this risk will determine the security measures required to protect the source. The higher the risk, the more capability will be required from the security systems.

This level of capability can be expressed as performance objectives on the security system. While there is a wide range of possible security measures, they can be described by their capability to deter, to detect and to delay unauthorized access or acquisition.

In TECDOC 1355 [13], four security groups are defined based on these fundamental protection capabilities. They provide a systematic way of categorizing the graded performance objectives required to cover the range of security measures that might be needed, depending on the assessed risk.

These security groups categorize the performance objectives of a security system as follows:

— **Security Group A:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible.

— **Security Group B:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner.

— **Security Group C:** Measures should be established to deter unauthorized access and verify the presence of the source at set intervals.

— **Security Group D:** Measures should be established to ensure safe use of the source and adequately protect it as an asset, verifying its presence at set intervals.

Table 1 provides a summary of these requirements.

5. ASSIGNMENT OF SOURCES TO GROUPS

The assignment of a radioactive source to a security group is most effectively achieved by using the outcomes of the threat assessment. This allows most flexibility and specificity to account for the variability in threat levels and security environments within Member States. It also permits different choices of security groups for sources in the different stages of their life cycle.

An alternative approach would be to base the security measures on the *consequences* of the malevolent acquisition and use of the source(s), and an assumed threat to the source. The IAEA has developed a revised Categorization of Radioactive Sources [11] that could be used for this first purpose, since it uses as its basis the potential human health impact of uncontrolled sources and provides a measure of the inherent hazard associated with the source. However, it should be recognized that it contains no consideration of the social or economic impacts of the loss of control of the sources.

In the revised categorization, sources are divided into five categories, with Category 1 being the most significant and Category 5 the least. Sources in Categories 1 to 3 generally have the possibility of giving rise to exposure sufficient to cause severe deterministic effects if they are uncontrolled. A severe deterministic effect is one that is fatal or life threatening or results in permanent injury that decreases the quality of life.

The security grouping of sources, given in Table 2, is based upon the revised categorization along with the implicit assumption of a threat by a person or group with serious intent to acquire the source. This latter assumption is used as a generic design basis threat. These assignments are put forward as default assignments. Different circumstances or more

detailed assessments may justify moving a source up or down a security group. One reason for a source being categorized in a higher security group could be that the specific threat assessment may reveal that some facilities with sources or some mobile sources are more vulnerable to acquisition, even though they may not be the highest activity sources.

However the assignment is made, either by use of threat assessment techniques or using the default assignment in Table 2, then it is possible to decide on some specific security measures that will meet the performance objectives for that group.

Two examples of this approach are given below.

Group A: Sources in storage

To achieve the defined performance objective, the following provisions could be implemented:

- a locked and fixed container or a device holding the source;
- a locked storage room, separating the container from unauthorized personnel;
- access control to the storage room;
- detection of unauthorized access or removal of the source;
- ability to respond in a timely manner to such detection.

For instance, if a high activity mobile source were in this group, the requirements could be:

- stored in a shielded container, which is locked;
- kept in an enclosed, secured vehicle;
- the vehicle parked inside a locked compound or locked garage;
- the vehicle subject to continuous detection of unauthorized intrusion attempts and there should be the capability to respond to intrusion.

These measures should provide the delay against the defined threat. Depending on the specifics of any threat assessment, additional responses might be required.

Group B: Sources in use

To achieve the defined objective, the following provisions could be implemented:

- use of the source in a locked room or controlled area;
- continuous surveillance of the source;
- access control to the room or controlled area.

For a mobile source, it is recognized that it might not always be possible to achieve the specified measures. Therefore, the vigilance of an administrative control such as personal surveillance needs to be rigorously maintained. Compensatory measures should also be considered to provide other levels of protection. These could include, for example, establishing a communication link to allow response to incidents, or potential threats. In addition, the required number of measures should be re-established as soon as possible after use.

All security measures should be scalable if a direct threat is received.

7. CONCLUSIONS

- Security of radioactive sources is a relatively new requirement to be added to the traditional focus on safety.
- Security measures need to balance with the need for availability
- The quality of the security measures needs to be commensurate with both the threat and the vulnerability
- A whole of lifecycle approach is needed to ensure security
- This is an international issue requiring efforts globally and involving manufacturers, regulators, users and governments

8. REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Goiânia, IAEA, Vienna (1988).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Tammiku, IAEA, Vienna (1998).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Lilo, IAEA, Vienna (2000).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Istanbul, IAEA, Vienna (2000).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Samut Prakarn, IAEA, Vienna (2002).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nature and Magnitude of the Problem of Spent Radiation Sources, IAEA-TECDOC-620, Vienna (1991).

[7] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, NUCLEAR ENERGY AGENCY OF THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT,

PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).
[8] KROCK, L., DEUSSER, R., Dirty Bomb — Chronology of Events, http://www.pbs.org/wgbh/nova/dirtybomb/chrono.html
[9] WALSH, N.P., Nick Paton Walsh in Moscow, The Guardian, 1 June 2002 (2002).
[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Revised Code of Conduct on the Safety and Security of Radioactive Sources, IAEA, Vienna (2003).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Revised Categorization of Radiation Sources, IAEA-TECDOC-1344, Vienna (2003).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA-TECDOC-1355, Vienna (2003).

Table 1. Summary of security group performance objectives

<table>
<tr><th>Security Group A</th><th>Security Group B</th><th>Security Group C</th><th>Security Group D</th></tr>
<tr><td colspan="4">Safe management and protect as an asset</td></tr>
<tr><td colspan="3">Deter unauthorized access</td><td rowspan="4"></td></tr>
<tr><td colspan="2">Timely detection of unauthorized access</td><td rowspan="3" colspan="2">Verification of source presence at set intervals.</td></tr>
<tr><td colspan="2">Timely detection of unauthorized acquisition of the radioactive source</td></tr>
<tr><td>Delay acquisition until response is possible</td><td></td></tr>
</table>

Table 2. Security groups based upon source categorization

Security Group	Source Category	Examples of practices
A	1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy Fixed multi-beam teletherapy (gamma knife)
B	2	Industrial radiography High/medium dose rate brachytherapy
	3	Fixed industrial gauges (e.g. level, dredger, conveyor) Well logging gauges
C	4	Low dose rate brachytherapy (except those below) Thickness/fill-level gauges Portable gauges (e.g. moisture/density) Bone densitometers Static eliminators
D	5	Low dose rate brachytherapy eye plaques and permanent implant sources X ray fluorescence devices Electron capture devices