Radiation Security

ATOMIC ENERGY LICENSING BOARD (AELB)
MINISTRY OF SCIENCE TECHNOLOGY AND INNOVATION

CATEGORIZATION SYSTEM

- The categorization is based on the concept of dangerous sources which are quantified in terms of D values.
- The D value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects.
- D values are used as normalizing factors to provide a reference for comparing risks.

EXPOSURE SCENARIOS USED IN DERIVING THE D VALUES

- An unshielded source (the D_1 value)
  - carried in the hand for one hour
  - carried in a pocket for 10 hours
  - being in a room for days to weeks
- Dispersal of a source by fire, explosion or human action (the D_2 value)
  - inhalation, ingestion and/or skin contamination

The lower value of D_1 and D_2 is used as the D value.

AELB ATOMIC ENERGY LICENSING BOARD

DOSE CRITERIA USED IN DERIVING THE D VALUES

Tissue	Dose criteria
Bone marrow	1 Gy in 2 days
Lung	6 Gy in 2 days from low LET 25 Gy in a year from high LET
Thyroid	5 Gy in 2 days
Skin/tissue (contact)	25 Gy at a depth of 2 cm (or 1 cm for the hand), for a period of 10 h
Bone marrow	1 Gy in 100 h for a source that is too big to be carried

EXAMPLES OF THE D VALUES

Radionuclide (TBq)	D Values
Am-241	0.06
Co-60	0.03
Cs-137	0.1
Ir-192	0.08
Pu-238	0.06
Sr-90	1.0
$Tc\text{-}99^{m}$	0.7

CATEGORIZATION SYSTEM

Initial ranking of sources:

- the activity (A) of a source is divided by the corresponding radionuclide specific D value.
- for commonly used sources the ratio A/D ranges from 10^{6} to 10^{-6}.

To obtain useful number of categories also other factors are considered:

- physical and chemical form
- type of shielding
- circumstances of use
- accident case histories

CATEGORIZATION SYSTEM (CONT)

- Five categories are introduced

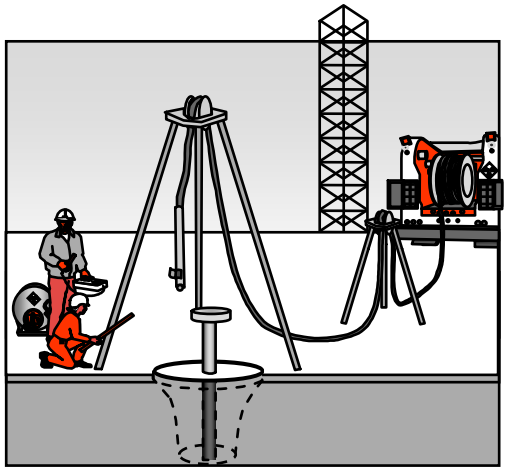
CATEGORY	ACTIVITY RATIO (A/D)
1	A/D ≥ 1000
2	1000 > A/D ≥ 10
3	10 > A/D ≥ 1
4	1 > A/D ≥ 0.01
5	0.01 > A/D and A > exempt

CATEGORY 3

10 > A/D ≥ 1

Examples :

- Fixed industrial gauges that incorporate high activity sources (Co-60, Cs-137)
- Well logging gauges (Cs-137, Am-Be)

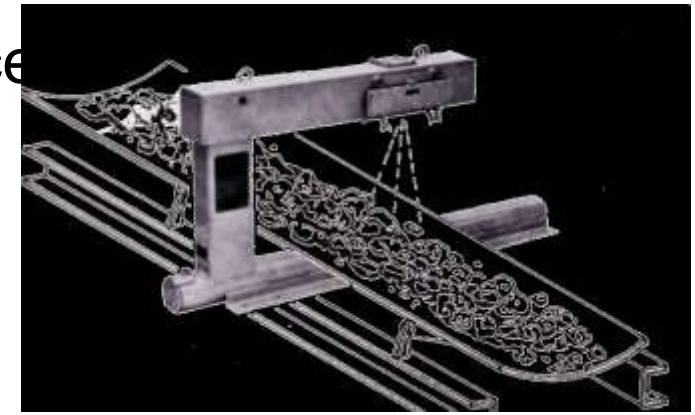


CATEGORY 4

1 > A/D ≥ 0.01

Examples :

- Low dose rate brachytherapy sources (except eye plagues and permanent implants)
- Industrial gauges that do not incorporate high activity source
- Bone densitometers
- Static eliminators



SECURITY GROUPING BASED ON SOURCE CATEGORIZATION (CONT)

Security Group	Source Category	Examples
A	1	• Irradiators • Teletherapy • Radioisotope thermoelectric generators • Fixed multi-beam teletherapy (gamma knife)

SECURITY GROUPING BASED ON SOURCE CATEGORIZATION (CONT)

Security Group	Source Category	Examples
B	2	• Industrial radiography • High/medium dose rate brachytherapy
	3	• Fixed gauges • Well logging

SECURITY GROUPING BASED ON SOURCE CATEGORIZATION (CONT)

Security Group	Source Category	Examples
C	4	• Low dose rate brachytherapy (except those in Security Group D) • Fill / Thickness gauges • Portable gauges (e.g. moisture / density) • Bone densitometers • Static eliminators

SECURITY GROUPING BASED ON SOURCE CATEGORIZATION (CONT)

Security Group	Source Category	Examples
D	5	• Low dose rate brachytherapy eye plaques and permanent implant sources • X-ray fluorescence devices • Electron capture devices

Sources Commonly Used In Gauging Activity For Category 3

Practice	Source/s
Level gauges	Cs-137, Co-60
Conveyor gauges	Cs-137, Cf-252
Blast Furnace Gauges	Co-60
Dredger gauges	Co-60, Cs-137
Spinning Pipe Gauges	Cs-137
Well Logging	Am-241/Be, Cs-137, Cf-252

Sources Commonly Used In Gauging Activity For Category 4

Practice	Source/s
Thickness Gauges	Kr-85, Sr-90, Am-241, Pm-147, Cm-244
Fill Level Gauges	Am-241, Cs-137, Co-60,
Moisture Detector	Am-241/Be
Density Gauges	Cs-137
Moisture/Density Gauges	Am-241/Be, Cs-137,

USE OF THE CATEGORIZATION SYSTEM (CONT)

Security measures

- To optimize security measures for radioactive sources, including measures directed against their possible malicious misuse.

USE OF THE CATEGORIZATION SYSTEM (CONT)

Labelling of high activity sources

- To guide decisions regarding which sources should be marked with an appropriate label warning of the radiation hazard.

USE OF THE CATEGORIZATION SYSTEM (CONT)

Emergency preparedness and response

- To ensure that emergency preparedness plans and response to accidents are commensurate with the hazards posed by the source.

USE OF THE CATEGORIZATION SYSTEM (CONT)

Emergency preparedness and response

- To ensure that emergency preparedness plans and response to accidents are commensurate with the hazards posed by the source.

USE OF THE CATEGORIZATION SYSTEM (CONT)

Emergency preparedness and response

Minimum contents of the plan

- Early notification procedures
- Immediate response measures to be taken
- Procedures for public communication

The plan should be

- Exercised periodically
- Evaluated periodically

SUMMARY OF EMERGENCY RESPONSE PLAN

CATEGORY	EMERGENCY RESPONSE PLAN
1	Specific plan
2	
3	
4	Generic plan
5	

USE OF THE CATEGORIZATION SYSTEM (CONT)

Communication with the public

- To provide a basis for explaining the relative hazard associated with events involving radioactive sources.
- Which is provides plain language descriptions of the categories for the purpose of public information.

COMMUNICATION WITH THE PUBLIC

Category	Risk in being close to an source
1	Extremely dangerous
2	Very dangerous
3	Dangerous
4	Unlikely to be dangerous
5	Most unlikely to be dangerous

LICENSEES RESPONSIBILITY

Licensees:-

- bear the responsibility for setting up and implementing the technical and organizational measures that are needed to ensure both the safety and security of the authorized sources.

- who appoint other people to carry out actions and tasks, nevertheless remain responsible for the relevant actions and tasks themselves.

LICENSEES RESPONSIBILITY

Licensees should ensure that sources are managed in accordance with the authorization:-

- when not in use, sources are promptly stored in an approved manner and relevant to the requirements of the category & security grouping to which the source(s) belong;
- the transfer of sources to another person is documented and that person is appropriately authorized to receive the transferred source;

LICENSEES RESPONSIBILITY

Licensees should ensure that:-

- financial provisions in accordance with regulatory requirements are in place for the safe disposal of disused sources

- sources are shipped and received in accordance with regulatory requirements

LICENSEES RESPONSIBILITY

The licensee must:-

- perform an inventory check of all radiation sources at regular intervals, including x-ray equipment, spent, calibration and crawler control radioactive sources.

- that all radioactive sources are surveyed when removed from, and returned to, storage.

LICENSEES RESPONSIBILITY

The licensee must:-

- apply the same survey and audit procedures to locations where extended field site work is taking place and where a temporary store is established.;

- if a radiation source cannot be located, take action as if an accident has occurred and shall immediately notify the Regulatory Authority.

LICENSEES RESPONSIBILITY

In addition to normal reporting requirements relating to safety issues, licensees should report to the Regulatory Authority:-

- any loss of control over a radioactive source;
- unauthorized access to, or unauthorized use of, a source;
- malicious acts threatening authorized activities;
- failures of equipment containing radioactive sources which may have security implications;
- the discovery of any unaccounted source.

SECURITY OF RADIOACTIVE SOURCES

AELB
ATOMIC ENERGY LICENSING BOARD

SAFETY

- Radiation safety was the prime focus, and the sources could be used for their intended beneficial purposes without harming either the user or the public.

- Safety deals with attempt to prevent/ minimize the exposure to radioactive sources, that may cause harm to human health.

  e.g Application of shielding when handling radioactive sources

SECURITY

- Security deals with attempting to prevent unauthorized or illegal acquisition and use of radioactive sources, with or without intention, including act for malevolent purpose.
  - e.g; CCTV at the radioactive sources storage facility
- Security failure, may lead to the safety incident/accident.
  - Gamma projector theft may lead to accidental radiation exposure to the public.

PURPOSE OF SECURITY MEASURES

To prevent

- Unauthorised access to radioactive sources at all stages of their life cycles (storage, use, transport, decommissioning and disposal)
- Damage to radioactive sources
- Loss of radioactive sources
- Theft of radioactive sources
- Unathorised transfer and use and of radioactive sources

SECURITY EVENTS INVOLVING RADIOACTIVE SOURCES

1.	**Missing Sources** (Medical) K.L	**1990s**
2.	**Sources Theft** (Industrial Radiography) Kuantan	**1990s**
3.	**Sources Theft** (Industrial Radiography) Taiping	**1990s**
4.	**Sources Storage Intrusion** (Industrial Radiography) Kemaman	**2001**
5.	**Sources Storage Intrusion** (Industrial Radiography) Miri	**2004**
6.	**Sources Storage Intrusion** (Industrial Radiography) Kemaman	**2006**
7.	**Missing Sources**(Oil Logging) Kemaman	**2007**
8.	**Sources Theft** (Industrial Radiography) Sibu	**2007**

PERFORMANCE OBJECTIVES

Security Level A	Security Level B	Security Level C	Security Level D
S			et
Det			
Timely detection acc			
Timely detection acquisition of the			urce presence at ervals
Delay acquisition until response is possible			

GENERAL RECOMMENDATION SECURITY MEASURES

Group A			Group D
Daily Accounting			Annual Accounting
Access Control to Source Location A of Unauthorized A			No Specific Provisions. Routine Measures to Ensure Safe Use and Protect as an Asset
Det			
Two Technical Measures Separating the Source from Unauthorized Personnel			
Specific Emergency Re			
Background Ch			
Security Plar			
Information Sec			
Upgrade Security for Inc			
Timely Detection Pro			
Remotely Monitored Intruder Alarm			
Timely Response to an Alarm			

APPLICABLE ADMINISTRATIVE MEASURES

Appropriate administrative measures include:-

- source inventories;
- regulations and guidance;
- reliability and trustworthiness of personnel;
- information security;
- quality assurance measures; and
- establishment of a safety culture and security culture.

TECHNICAL MEASURES

Measures that pose a physical barrier to the source, device or facility

- To separate it from unauthorized personnel
- To deter or prevent unauthorized access or removal of a source

APPLICABLE TECHNICAL MEASURES

Appropriate technical measures include:-

- fences;
- walls;
- cages;
- transport packaging;
- locks and interlocks for doors (or access points)
- locked, shielded containers;

Recommended Measure For Security Level B

(goal : minimize the likelihood of unauthorized removal)

Security Function	Security Objectives	Security Measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronics intrusion detection equipment and/or continuous surveillance by operator personnel
	Provide detection of any attempted unauthorized removal of the source	Tamper detection equipment and/or periodic checks by operator personnel
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator/response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phone, pagers and radios
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper detection equipment, etc

Recommended Measure For Security Level B

(goal : minimize the likelihood of unauthorized removal)

Security Function	Security Objectives	Security measures
Delay	Provide delay to minimize the likelihood of unauthorized removal	System of two layers of barrier (technical measures) such as walls, cages etc
Response	Provide immediate initiation of response to interrupt unauthorized removal	Equipment and procedures to immediately initiate response

Recommended Measure For Security Level B

(goal : minimize the likelihood of unauthorized removal)

Security Function	Security Objective	Security Measures
Security Management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measures
	Ensure trustworthiness of authorized individuals	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide security plan	A security plan which conforms to regulatory requirements and provides for response to increase threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security related scenarios
	Establish security event reporting system	Procedures for timely reporting of security events

Recommended Measure For Security Level C

(goal : reduce the likelihood of unauthorized removal)

Security Function	Security Objectives	Security Measures
Detect	Provide detection of unauthorized removal of the source	Tamper detection equipment and/or periodic checks by operator personnel
	Provide immediate assessment of detection	Assessment by operator/response personnel
	Provide a means to detect loss through verification	Monthly checking through physical checks, tamper indication devices, or other checks to confirm the presence of the source

Recommended Measure For Security Level C

(goal : reduce the likelihood of unauthorized removal)

Security Function	Security Objectives	Security measures
Delay	Provide delay to reduce the likelihood of unauthorized removal of a source	One barrier (technical measures) such as walls, cages, source housing or under observation by operator personnel
Response	Implement appropriate action in the event of unauthorized removal of a source	Procedures for identifying necessary actions in accordance with contingency plan

Recommended Measure For Security Level C

(goal : reduce the likelihood of unauthorized removal)

Security Function	Security Objective	Security Measures
Security Management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measures
	Ensure trustworthiness of authorized individuals	Appropriate methods for determining the trustworthiness of unauthorized individual with unescorted access to radioactive sources and access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide security plan	Documentation of security arrangements and reference procedures
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security related scenarios
	Establish security event reporting system	Procedures for timely reporting of security events

Thank you