SAND2007-1278 C

SAND2007-1278C

Radioactive Source Security Awareness Seminar

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Welcome and Opening

CAEA

Introductions

Mark Soo Hoo
Sandia National Laboratories
mssooho@sandia.gov

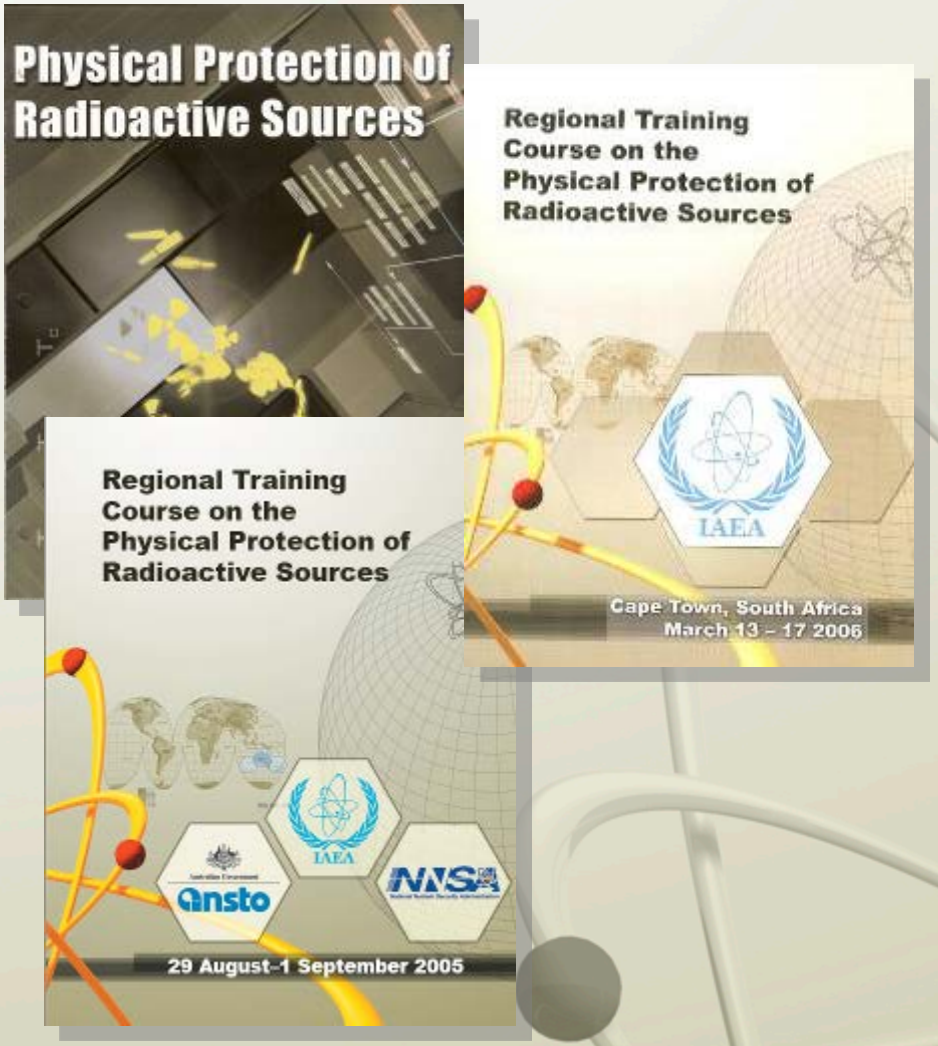
Keith Young
Sandia National Laboratories
kayoung@sandia.gov

Guy Jones
Sandia National Laboratories
gbvarna@sandia.gov

Chris Behan
International Atomic Energy Agency
c.behan@iaea.org

Seminar and Workshop Overview

- 1-day seminar (Protection of Radioactive Sources)
- 3-day workshop (DBT)
- Materials developed for DOE National Nuclear Security Administration (NNSA) and presented internationally
- Developed in cooperation with the IAEA



Questions are welcome at any time

Radioactive Source Security Seminar Objectives

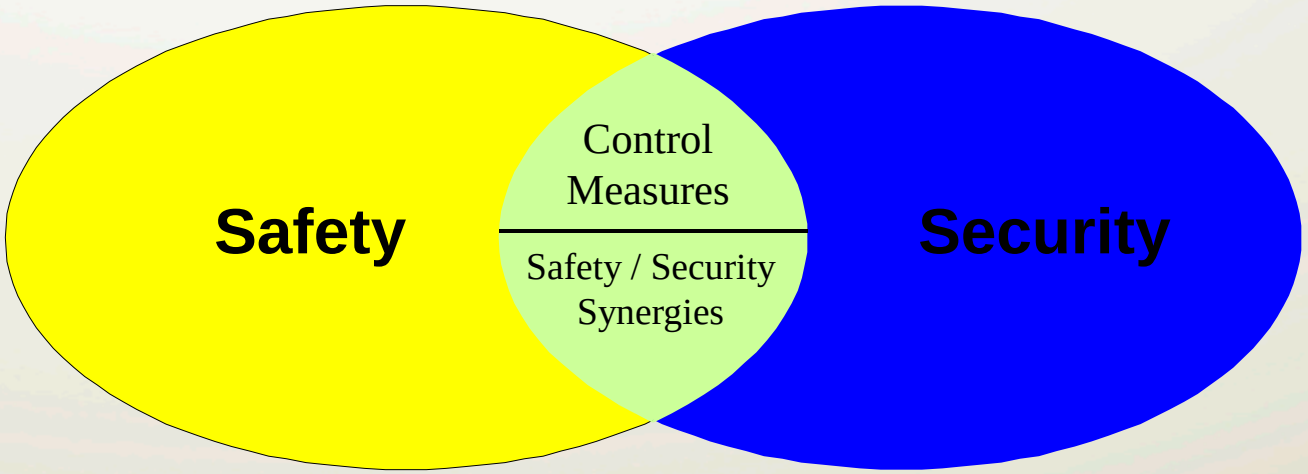
1. Create awareness of the need to protect and control sources and apply adequate physical protection measures to sources throughout their life cycle
2. Describe international recommendations and physical protection principles, and provide a basic understanding of physical protection systems for radioactive sources
3. Provide an overview of the practical aspects of regulating radioactive source security

Radioactive Source Security Seminar Agenda

- Need for Source Security
- IAEA Source Security Initiative
- Source Security in China
- Source Characterization
- Physical Protection Systems
- Security of Radioactive Sources
- Examples of Physical Protection Systems
- Discussions
- Closing

- The Need for Source Security
  - The global threat
  - Ease of access to unsecured sources
  - Potential malicious acts and their consequences

Safety and Security



Radiation Safety
- **Intrinsic to activity**
- **Probabilistic analysis**
- **Transparency**

Regulatory Infrastructure
Categorization of Sources
Orphan Source Recovery
Emergency Response Plans
Radioactive Waste Management
Safety engineering and source Design

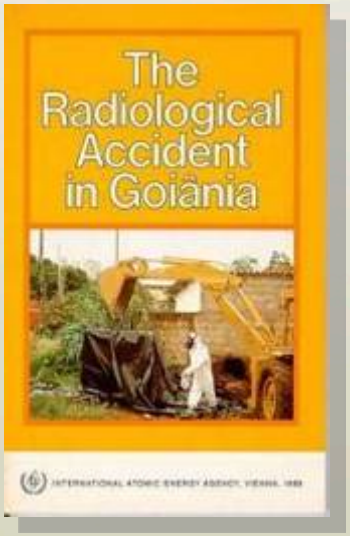
Source Security
- **Malevolent activity**
- **Threat-based judgment**
- **Confidentiality**

Loss of Control of Radioactive Source

SAFETY

Inadvertent loss or damage

- Misplaced
- Forgotten
- Accidents



SECURITY

Intentional

Damage

- Sabotage

Acquisition

- Theft
- Illegal purchase
- Legal purchase

Malicious motive

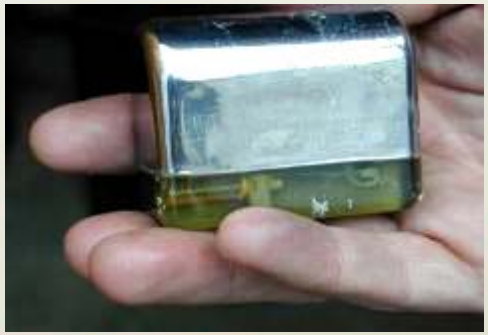
- Terrorism
- Individual's intent to harm other(s)

Financial motive

- Illegal sale for profit
- Avoidance of costs of ownership
- Extortion

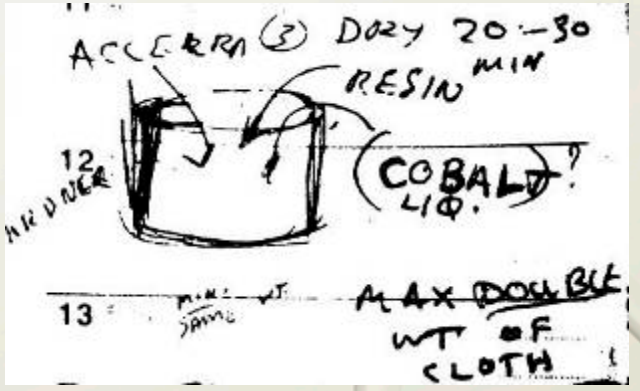
Malicious Use of Radioactive Material

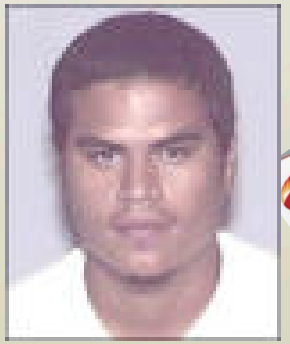
- Readily available material
- Relatively unsophisticated technology
- Minimal security in many instances
- Cause fear and panic
- Results in area denial, disruption, and economic impact



A Matter of When, Not If

- 1987—Iraq tested RDD
- 1995—RED discovered in Moscow Public Park
- 1998—Chechnya: Explosive mine filled with radioactive material
- 2002—Jose Padilla found to have plans
- 2003—Al Qaeda plans in Afghanistan
- 2004—Large stockpile of Americium 241 found in London





Article Published on Bin Laden Web Site

http://www.israelnewsagency.com/binladenislamicnuclearterror.html

الحرب النووية هي الحل لتدمير أمريكا

بسم الله الرحمن الرحيم

نعم لم تخطئوا قراءة النص ،إنه السبيل الوحيد لقتل أكبر عدد ممكن من الأمريكان ،إنه الرعب النووي الذي لا يخشى الأمريكان مثله أبداً ففي الحرب العالمية الثانية استخدمت أمريكا هذا السلاح مرتين خلال ثلاثة أيام بسبب الغارة اليابانية الناجحة على بيرل هاربر ،والآن تقوم الولايات المتحدة الأمريكية باستخدام أعنف الأسلحة وأشدها فتكاً وتطوراً في قصف المدنيين الآمنين في العراق ،والمدنيين الآمنيين في أفغانستان وتدعم وبكل فخر الحرب الروسية ضد الشيشان ،ليس حباً في الروس ولكن بغضاً في المسلمين .

لقد قصفت أمريكا العراق بأسلحة لوثت الأرض والماء الجوفية بالإشعاع لآلاف السنين، بل قد قامت بإشاعة التخلف بالبور اليوم المستلفد لكي توقع أكبر ضرر في الأرض والإنسان، حتى تخرج من جزيرة محمد ،وقد حولتها إلى منطقة محرمة فلا يفكر أحد بعد ذلك في العجز إليها ،و لكن يبدو أن حيوانات البيت الأبيض نسوا أو تناسوا شيئ هاماً للغاية ،هذا الشئ هو ويكل الفخر والاعتزاز «بتنظيم القاعدة».

هذا التنظيم الذي أثار الرعب في قلب الغرب الكافر ،وجعل من بضع شباب لا يملكون من الدنيا إلاّ حبهم لله ولرسول تكالاً في إبقاء المومسات، بل لقد صدر هؤلاء الشباب لروح الأمثلة في تعففهم للدنيا ،فقد أنفقوا الدنيا وفروا منها لايلون شيئ سوى رضاهم بما عند الله تعالى ،فباعوا النفسهم لله ،والله ثم بهم وتقبله.

إذاً فالعالمين بالعين والسن بالسن ،وإذا كان الأمريكان يمتلكون القنابل التي لاتقبل لا حد بها ،فالقاعدة تملك من القنابل التي تسمى «بالقنابل القذرة» و «القنابل الفايروسات القاتلة» ، التي ستشمل المدن الأمريكية بالأمراض القاتلة لتحول هذا الشعب «المتأنق والمتغطرس في إذلال الشعوب الأخرى» إلى شعب من المنبوذين المحاصين للأمراض وستثبت الأيام القادمة أن قاعدة الجهاد بإذن الله تعالى قادرة على تحويل أمريكا إلى بحيرة من الإشعاع القاتل ،الذي سوف يثبت للعالم أقرب النهاية ،وسوف يثبت أيضاً أن القاعدة ستكون عند حسن ظن العالم الإسلامي بها من القضاء على أمريكا .

نعم ستدمر أمريكا ومن تحالف معها ،لأنهم تمادوا استخدام القوة ضد الضعفاء ،والآن اقتربت نهايتهم على يد شباب الصحوة الذين إن ركبوا خيولهم لايعودون عنها إلا منتصرين أو شهداء بإذن الله ،وكلتا الحالتين نصر مؤزّر .

فأكثروا من الدعاء لإخوانكم بالتسديد والنصر والله القادر على كل شئ.

هذا بيان للناس ليتفقه فيه المؤمنون فقط أما الكافرين فإنا نسأل الله تعالى أن يهديهم أو أن يعجّل في قبض أرواحهم وأما عدوّنا فالله سبحانه عليه.

والله من وراء القصد وهو أرحم الراحمين .

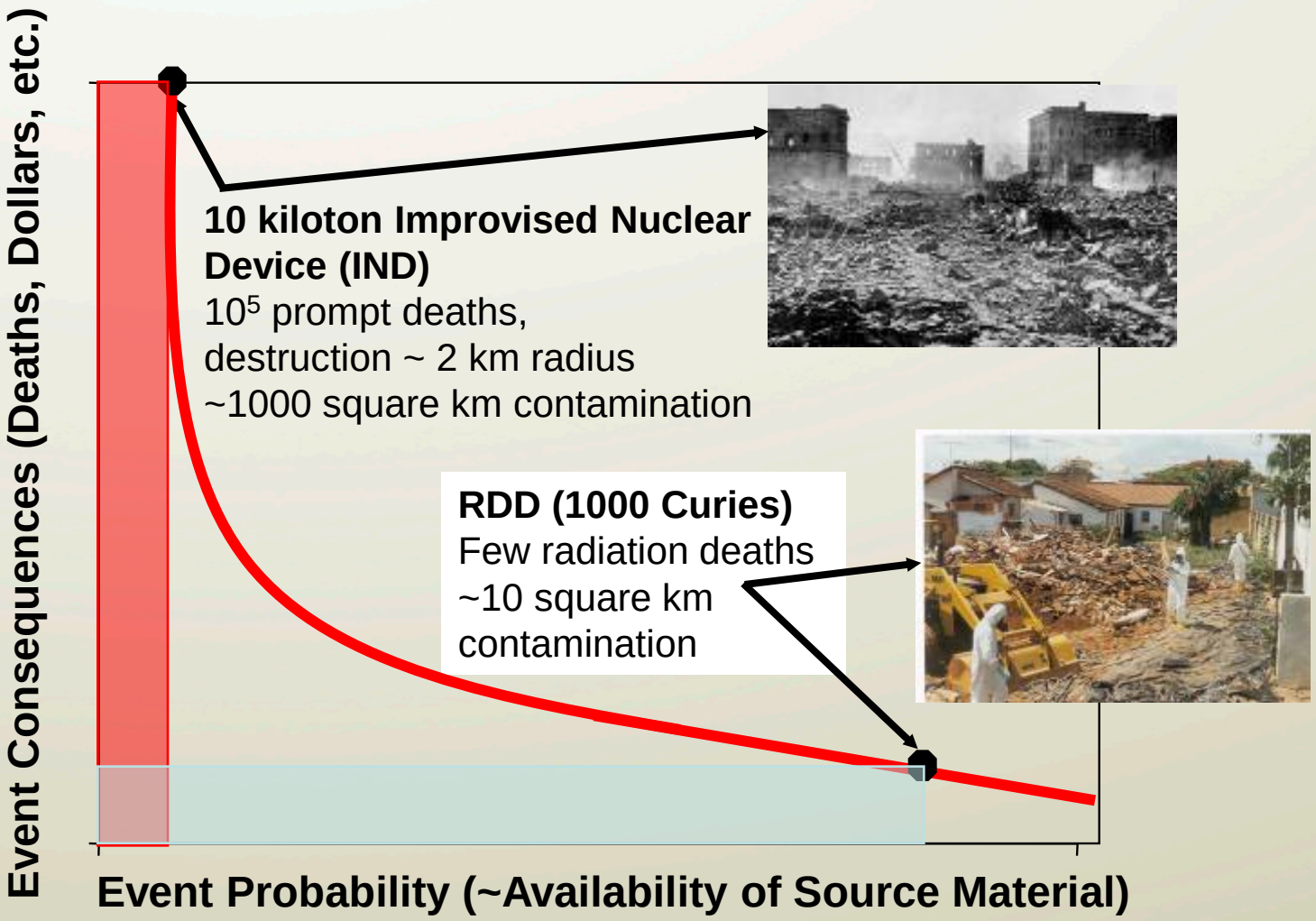
منقول

«أبو شهاب القندهاري»

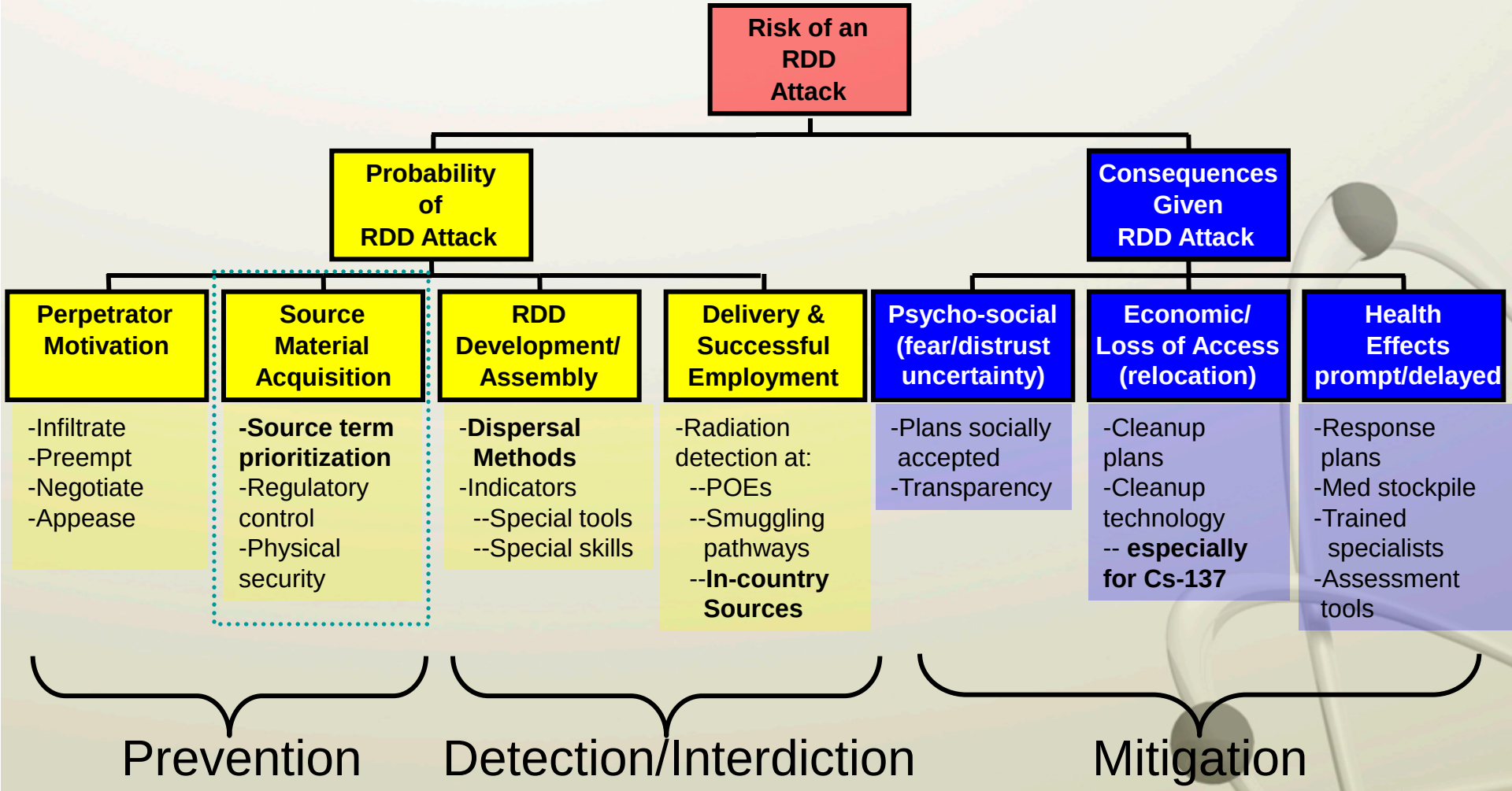
تم تحرير هذا المقال في 02-12-26 عند 07:00 AM

"Even though the Americans have bombs possessing enormous power, Al-Qaeda is even more powerful than they, and it has in its possession bombs which are called "dirty bombs"

RDD Risk in Perspective:
Risk = Probability x Consequences



The RDD Risk Equation and Risk Reduction Countermeasures

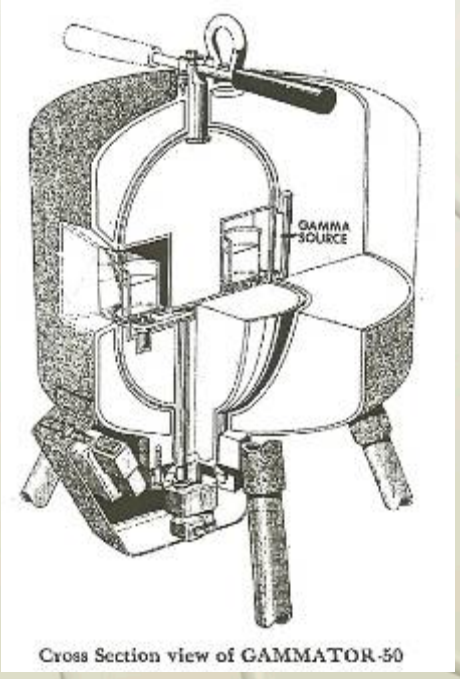


Abandoned Sources

Vulnerable Sources and Devices

Availability

- “To all licensees, here at the University of ------, one of our responsible users would like to offer up a self-shielded irradiator for recycling. … Specifications: Isomedix (Parsippany, N.J.) Gammator M38-1 irradiator; Two source Cs-137 Reference date and reference activity 7/1/1969 800 Ci (400 Ci/source) Current activity and exposure rate 360 Ci 309 R/min. The two sources are contained within two welded, stainless steel concentric capsules locked in a third cavity by a shielding plug which is locked into place by a high strength weld.”
- On a high school website: “In a specially constructed room in the main lab, we maintain a Model B Gammator Irradiator with a 400 curie source of Cs-137. For this the school is licensed by the State, and I am named as the control operator on the license. The gammator is used by students to irradiate everything from seeds to non-living materials.”



Cross Section view of GAMMATOR-50

Availability

Re: Cobalt-60 Gamma Irradiator
To: radsafe@********
Subject: Re: Cobalt-60 Gamma Irradiator
From: John ***** <jm***r@********>**
Date: Thu, 16 Dec
We have an AECL Gamma Cell 220 with about 900 Ci of Co-60. … Has anybody had experience getting rid of this much Co-60 or an irradiator?

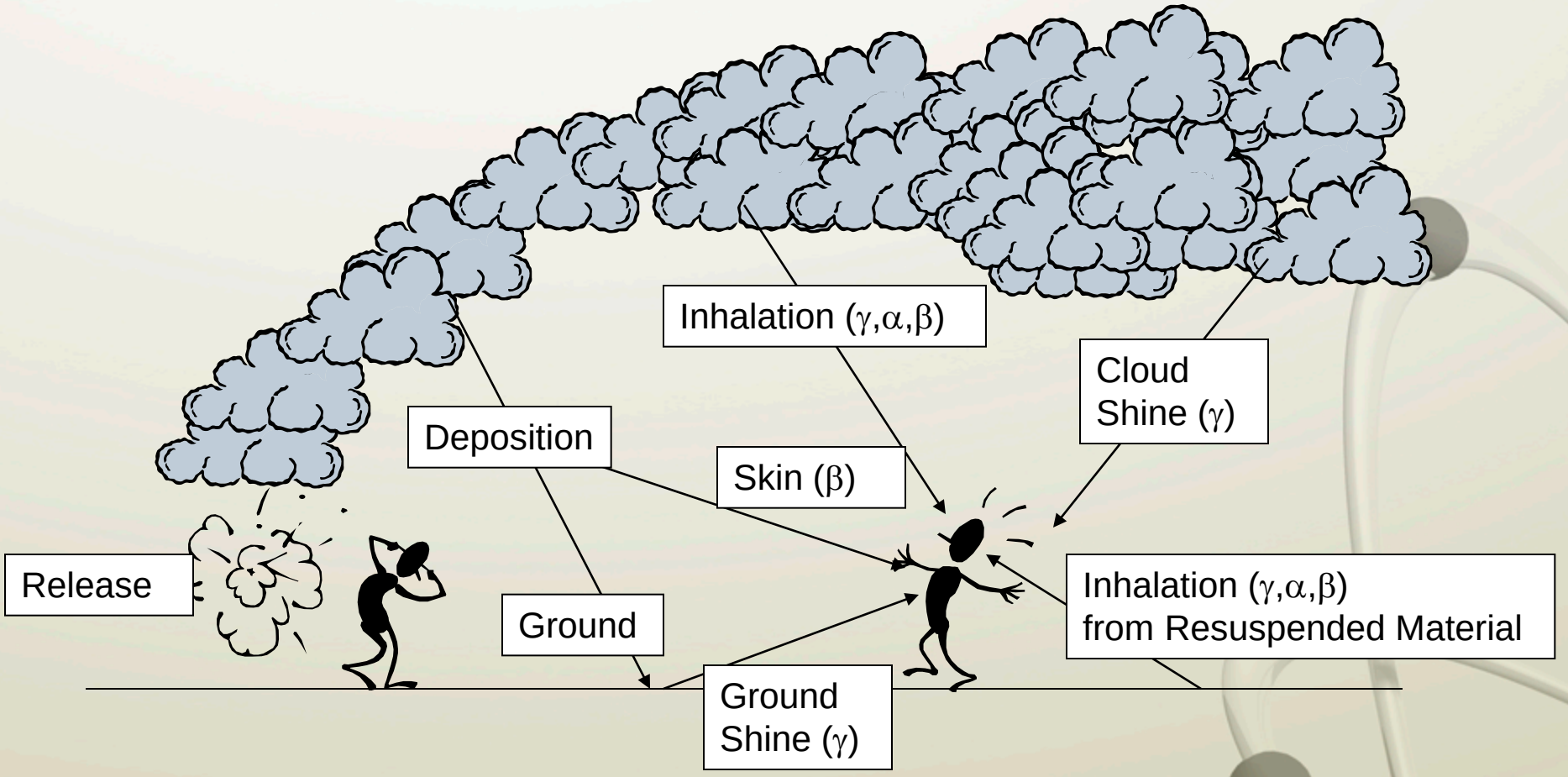
I am storing a RAMCO (Radiation Machinery Co.) GAMMATOR 50. This source currently contains approximately 200 curies of Cs-137-Cl. This source is free to anyone who has a license and can remove it from our site

supply of cobalt-60 source for NDT
Posted by: John H****** , E-mail: j*******g@comcast.net, on September 09:
We have Cobalt-60 nickel plated 1 x 1 mm pallet with high activity of 250 - 300 Ci/g suitable for the application of NDT or Gamma Knife. We have hot cell at the lab in China to process the Co-60 into source per customers' requirement as OEM. If anyone in this forum is interested, please contact me.

Price: £340.00

Nuclear Isotopes
Radioactive Sources
No NRC license required!

Major Pathways from Release



Consequences of Malicious Use of Sources

- Likely consequences of malicious use
- Types of events of concern
- Assessment of consequences
- The consequences of a major incident

What are the most likely events of concern?

- Sabotage
- Theft and dispersal; for example, through use in
  - Radiological Exposure Device (RED)
  - Radiological Dispersion Device (RDD)

What are the possible consequences of the malicious use of sources?

- Acute radiation sickness or fatality
- Radiation dose to the public and emergency workers with subsequent increase in latent cancer fatality
- Contamination
- Loss of function (area or facility)
- Economic disruption
- Social disruption
- Psychological effects

Level of Harm—Consequences

Level of consequence may be determined by:

- Type of event
- Exposure and contamination
- Cultural and political issues
- Emergency response

Level of Harm—Consequences

Exposure and contamination:

- How many people exposed?
- Duration of exposure?
- Dominance of exposure and contamination pathways—external or ingestion or inhalation

Level of Harm—Consequences

Cultural and political issues:

- What is the number of “acceptable” casualties from a terrorist attack?
- What is an acceptable level of residual radiation after contamination?

Level of Harm—Consequences

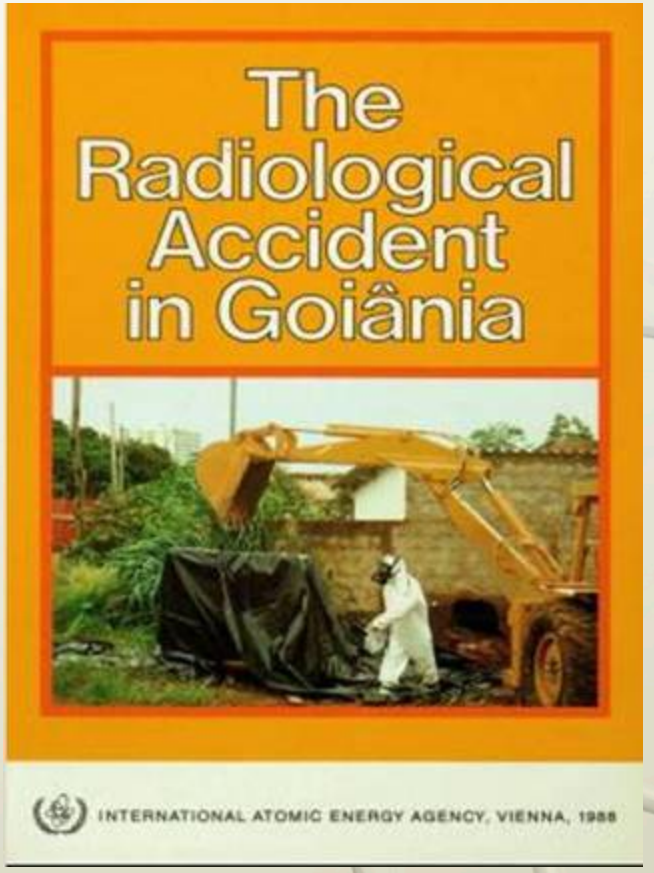
Emergency response:

- An RDD may initially appear to be a conventional bombing
- Ability to respond to an RDD attack to limit contamination spread, monitor radiation exposure, etc.

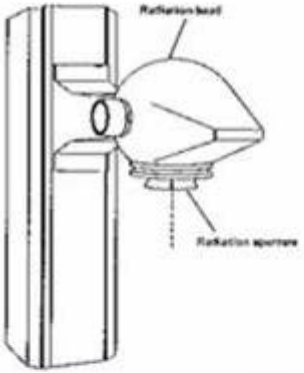
Consequences of the Goiânia Accident

A benchmark for consequences caused by a breach in security?

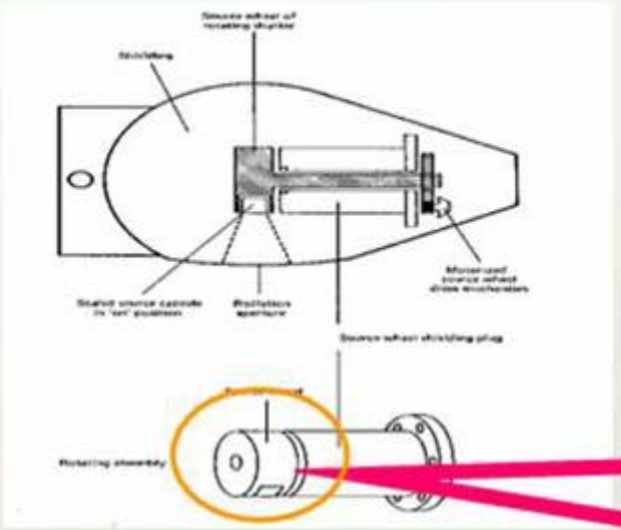
- Unsecured Cs-137 source in radiological clinic
- Category 1 source
- Scrap scavengers stole housing (lead shielding) and sold it to junkyard
- Radioactive source was cut open with plasma torch



The Goiânia Accident



Caesium-137
Teletherapy Unit



Teletherapy Source and shielding

Source
~ 2.5 cm dia.
~ 1400 Ci, Cs-137
CsCl salt (powder)

Source

The Goiânia Accident:
Area Contaminated = 1km^2

A: IGR clinic
B: Source first exposed
C: Junkyard I
D: Junkyard II
E: Junkyard III
F: Vigilância Sanitária
G: Physicist W.F.'s house
H: Olympic stadium
J: General Hospital
K, L: Other contamination points
M: Initial CNEN command post
N: Present CNEN office

FIG. 7. Plan of Goiânia showing the principal sites of contamination.

The Goiânia Accident: Social Disruption

- 159 houses monitored, 101 houses contaminated
- 200 persons evacuated from 41 of the houses
- 42 houses decontaminated, 6 demolished
- 58 different public places decontaminated, including streets, shops, bars, and 64 vehicles

13. Contaminated rubble from the demolition of R.A.'s house on 57th Street.

14. The same site after removal of the contaminated rubble.

The Goiânia Accident: 3500 Cubic Meters of Waste

An estimated 16 g of Cs-137 was released passively and generated 40 tons of radioactive waste

- 3800 metal drums (200 L)
- 1400 metal boxes (5 tonnes)
- 10 shipping containers (32m^3)
- 6 sets of concrete packaging

27. Waste containers at the temporary storage site.

The Goiânia Accident: Impact to the Local Population

- Population 1 million
- Persons monitored 112,800
- Persons contaminated
  - Clothes and shoes 120
  - Skin and internally 151
- Radiation injuries 28
- Hospitalized 20
- Bone marrow depression 14
- Acute radiation syndrome 8
- Fatalities within one month 4

The Goiânia Accident: Economic Impact

- Initial response lasted for 6 months
- Around $20–35 million spent
- 730 workers involved in decontamination activities
- 10 years for city to recover to pre-incident economic levels

The Goiânia Accident: Psychological Effects

The Need for Radioactive Source Security—Summary

- The threat is real
- Sources must be secured to prevent their use in malicious acts
  - Orphan sources
  - Sources in use and storage
- Likely consequences of malicious use are severe
- Source security should be a priority for all licensees

Chris Behan

- Greece Olympics

Chris Behan

- IAEA Source Security Initiative
  - Background
  - Code of Conduct on the Safety and Security of Radioactive Sources

Emergence of Source Security as an International Priority

United Nations

Security Council

Resolution 1373 (2001)

Adopted by the Security Council at its 4385th meeting, on 28 September 2001

The Security Council,

Reaffirming its resolutions 1269 (1999) of 19 October 1999 and 136[illegible] 12 September 2001,

Reaffirming also its unequivocal condemnation of the terrorist atta took place in New York, Washington, D.C. and Pennsylvania on 11 Septe and expressing its determination to prevent all such acts,

Reaffirming further that such acts, like any act of international constitute a threat to international peace and security,

Reaffirming the inherent right of individual or collective self-d recognized by the Charter of the United Nations as reiterated in resolu (2001),

Reaffirming the need to combat by all means, in accordance with the the United Nations, threats to international peace and security caused b acts,

Deeply concerned by the increase, in various regions of the world, terrorism motivated by intolerance or extremism,

Calling on States to work together urgently to prevent and suppre acts, including through increased cooperation and full implementati relevant international conventions relating to terrorism,

Recognizing the need for States to complement international coop taking additional measures to prevent and suppress, in their territories t lawful means, the financing and preparation of any acts of terrorism,

Reaffirming the principle established by the General Assem declaration of October 1970 (resolution 2625 (XXV)) and reiterated by th Council in its resolution 1189 (1998) of 13 August 1998, namely that e has the duty to refrain from organizing, instigating, assisting or partic terrorist acts in another State or acquiescing in organized activities territory directed towards the commission of such acts,

Acting under Chapter VII of the Charter of the United Nations,

International Atomic Energy Agency

BOARD OF GOVERNORS

GENERAL CONFERENCE

B

GC

NUCLEAR SECURITY – PROGRESS ON MEASURES TO PROTECT AGAINST NUCLEAR TERRORISM

International Conference on Security of Radioactive Sources

Vienna, Austria

10-13 March 2003

CODE OF CONDUCT ON THE SAFETY AND SECURITY OF RADIOACTIVE SOURCES

放射源安全和保安行为准则

CODE DE CONDUITE SUR LA SÛRETÉ ET LA SÉCURITÉ DES SOURCES RADIOACTIVES

КОДЕКС ПОВЕДЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ И СОХРАННОСТИ РАДИОАКТИВНЫХ ИСТОЧНИКОВ

CÓDIGO DE CONDUCTA SOBRE SEGURIDAD TECNOLÓGICA Y FÍSICA DE LAS FUENTES RADIACTIVAS

مدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها

IAEA International Atomic Energy Agency

Code of Conduct

- Approved by the IAEA Board of Governors on 19 September 2003
- Replaces previous version published in March 2001
- Issued in six languages, including English and Spanish

Scope

- Focuses on Category 1, 2, and 3 sources, which were identified in Annex 1
- “In addition to these categories, States should give appropriate attention to sources [which could cause] unacceptable consequences if used for malicious purposes”
- Excludes special nuclear material (except for Pu-239/Be sources)
- Excludes radioactive sources within the military or defense programs

Objectives

- Achieve and maintain a high level of safety and security of radioactive sources
- Prevent unauthorized access or damage to and loss, theft, or unauthorized transfer of radioactive sources, and prevent the malicious use of radioactive sources to cause harm to individuals, society, or the environment
- Mitigate or minimize the radiological consequences of any accident or malicious act involving a radioactive source

Target Audience

- Designed primarily for national governments
- Provides guidance for legislation, regulations and the regulatory body in order to:
  - Ensure that sources are safely managed and securely protected during and at the end of their useful lives
  - Establish an effective national legislative and regulatory system of control, with primary responsibility on the persons authorized to manage sources

Status

- Not legally binding
- General conference resolution GC(47)/RES/7.B urges each Member State to write to the Director General that:
  - it fully supports and endorses the IAEA's efforts to enhance the safety and security of radioactive sources, and
  - is working toward following the guidance contained in the Code and is encouraging other countries to do the same
- As of 15 November 2006, 88 countries have submitted such letters (including Mexico and the United States)
- Country list available at:

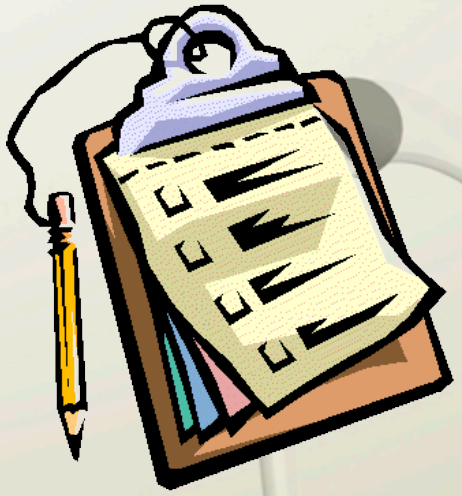
  http://www.iaea.org/Publications/Documents/Treaties/codeconduct_status.pdf

Code of Conduct Contents

- **Foreword** explaining the history and development of the Code
- Considerations in the development of the Code
- Pertinent **Definitions**
- **Scope and Objectives**
- **Basic Principles**, including:
  - General source safety and security elements
  - Key areas of focus for source safety and security:
    - Legislation and Regulations
    - Regulatory Body
    - Import and Export of Radioactive Sources

Key Provisions

- Effective national legislative and regulatory system of control
- Effectively independent regulatory body to establish and enforce security requirements
- Prime responsibility for security on licensee
- Promotion of security culture
- National registry of sources
- Regular inventory controls by licensee
- States should define domestic threat and assess vulnerability



Key Provisions (continued)

- Security measures to deter, detect, and delay theft or removal of sources
- Assessment of the security of the source and/or facility
- Verification of safety and security
- Prompt reporting by licensee of loss of source control
- Safe management and secure protection of disused sources
- Import and export controls

Import/Export Controls

- Import and export of Category 1 and 2 radioactive sources should take place only with the *prior notification* by the exporting state and, as appropriate, consent of the importing State
- Importing State should consent only if the *recipient is authorized* under its national legislation to receive the source

Import/Export Guidance

- *Code of Conduct on the Safety and Security of Radioactive Sources: Guidance on the Import and Export of Radioactive Sources*
- Approved 14 September 2004 by the IAEA Board of Governors
- 37 countries have submitted letters support to the IAEA, as of 15 November 2006 (including Mexico and the United States)

Import/Export Guidance (cont'd)

- Provides guidance on how to import and export Category 1 and 2 sources in accordance with the Code of Conduct
- Encourages each state to nominate a Point of Contact to facilitate imports and exports (CNSNS in Mexico, NRC and DOE in the United States)
- Explains terminology pertaining to import and export of sources not given in the Code
- Defines "exceptional circumstances" when import or export may be authorized even though import-export guidance cannot be followed
- Includes a State Self-Assessment Questionnaire regarding the State's regulatory framework

Summary

- The Code of Conduct provides guidance to Member States for the development and harmonization of policies, laws and regulation to establish the safety and security of radioactive sources
- Guidance developed for import/export
- To date, 88 Member States have written letters to the IAEA expressing support for the Code of Conduct

NNSA/SEPA

- Source Security in China
  - Regulatory structure
  - Regulations and guidance

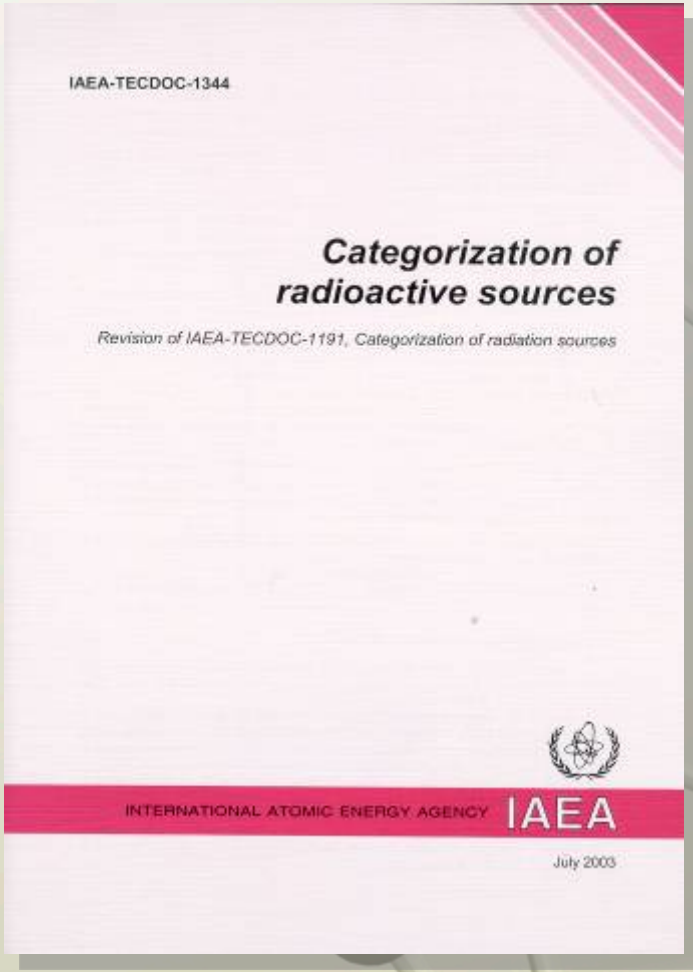
- Source Characterization
  - TECDOC 1355
  - NNSA Program Thresholds
  - Other approaches

Code of Conduct on the Safety and Security of Radioactive Sources

- International guidance to achieve and maintain a high level of safety and security of radioactive sources
- Applies to Category 1, 2, and 3 sources, as defined in Safety Guide RS-G-1.9, Categorization of Radioactive Sources

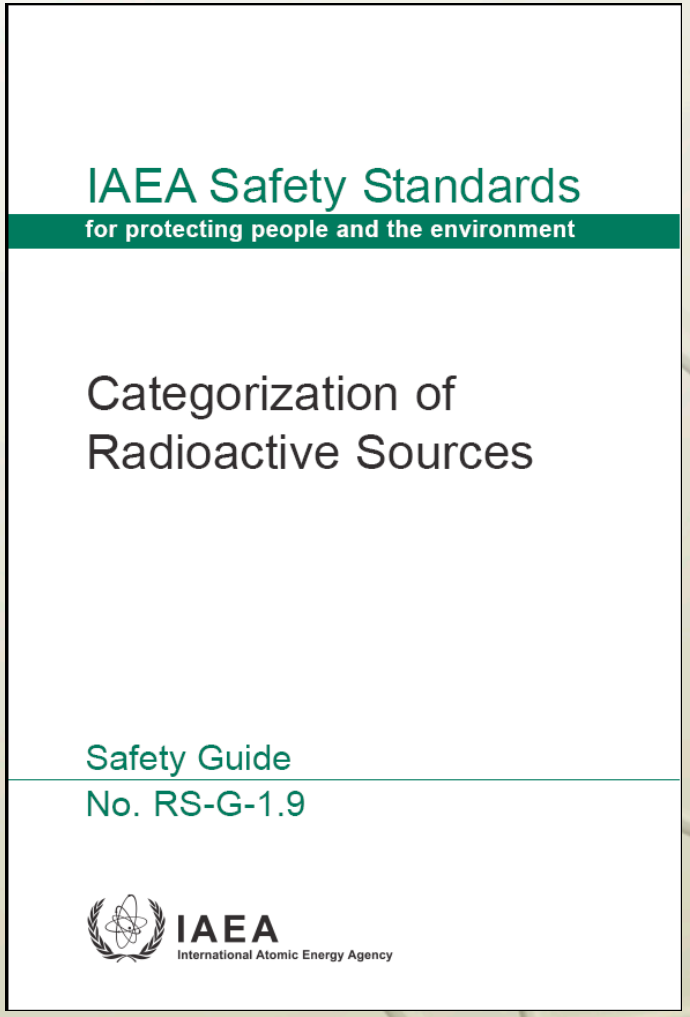
Categorization of Radioactive Sources (TECDOC-1344)

- Assigns radioactive sources into five categories
- Envisions application for a variety of purposes
  - Regulatory measures
  - Security measures
  - National source registries
  - Import-export controls
  - Labeling
  - Emergency preparedness
  - Orphan source recovery
  - Communications with the public



Categorization of Radioactive Sources (Safety Guide RS-G-1.9)

- Published August 2005
- Essentially the same as TECDOC-1344, except:
  - Inclusion of *Implementation of the Categorization System* in Section 3, including *National Register of Radioactive Sources* discussion in Section 3.7
  - Differentiation of source activity for industrial gauges in Categories 3 & 4
  - Refined Rationale and Method for the Categorization of Radioactive Sources included as Annex I
  - Inclusion of specific references for *D* Value in Annex II



Basis of Categorization in Safety Guide

- Based on the potential for sources to cause harm to human health
- Determined by the “Activity Ratio,” A/D, where:

  A = the activity of a source material in a given practice

  D = the value which will yield pre-defined (deterministic) dose consequences (reference Safety Guide Annex II).

D-Value Includes Internal and External Exposure

Internal exposure

- Inadvertent intake following dispersion e.g., ingestion, inhalation, etc.

External exposure

- Unshielded source in pocket, hand, or room
- Skin contamination

Examples of severe deterministic effects from ‘Dangerous Sources’

Summary Table

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≥ Exempt/D

Categorization Method

- A/D ratios are calculated for radionuclides in a variety of practices
- The assignment of radionuclides to categories is further refined based on other factors, such as:
  - physical and chemical form
  - source shielding
  - circumstances of source use
  - accident case histories

Categorization Table 1

Category	Sources and Practice
1	RTGs, Irradiators, Teletherapy sources, Fixed multi-beam teletherapy (gamma knife) sources
2	Industrial gamma radiography sources, High/medium dose rate brachytherapy sources
3	Fixed industrial gauges that incorporate high activity sources, Well logging gauges
4	Low dose rate (LDR) brachytherapy sources, Industrial gauges that do not incorporate high activity sources, Bone densitometers, Static eliminators
5	LDR brachytherapy eye plaques and permanent implant sources, X-ray fluorescence devices, Electron capture devices, Mossbauer spectrometry, Positron emission tomography (PET) check sources

Example

- Device: Blood/Tissue Irradiator
- Radionuclide: Cs-137
- Typical Quantity in Use (A): 260 TBq
- D-Value: 0.1 TBq
- Ratio of A/D = 260/0.1 = 2600
- A/D-Based Category: 1 (A/D ≥ 1000)
- Assigned to Category 1

Other Cases

- Practices Unknown or Not Listed in Table 1
  - Calculate A/D Ratio
  - Assign category based on A/D ratio, considering other applicable factors
- Short half-life and unsealed sources
  - Need to use judgment in selecting the activity to calculate A/D
  - Should be considered on a case-by-case basis

Aggregate Sources

- Multiple sources in close proximity in a single storage or use location
- If sources with a single radionuclide are aggregated, sum the total activity, A, and divide by D to calculate the A/D Ratio
- If sources with several radionuclides are aggregated, use the following formula:

$$\text{Aggregate A/D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

Where:

$A_{i,n}$ = Activity of Each Individual Source, *i*, of Radionuclide, *n*

D_n = D Value for Each Radionuclide, *n*

Categorization and Security

- Categorization in the Safety Guide is based on the potential of sources to cause harm to human health.
- *However*, the categories are envisioned to be applied to many situations, including provision of a graded basis for assisting in the choice of security measures, along with other factors such as threat.

Categorization and Security (cont'd)

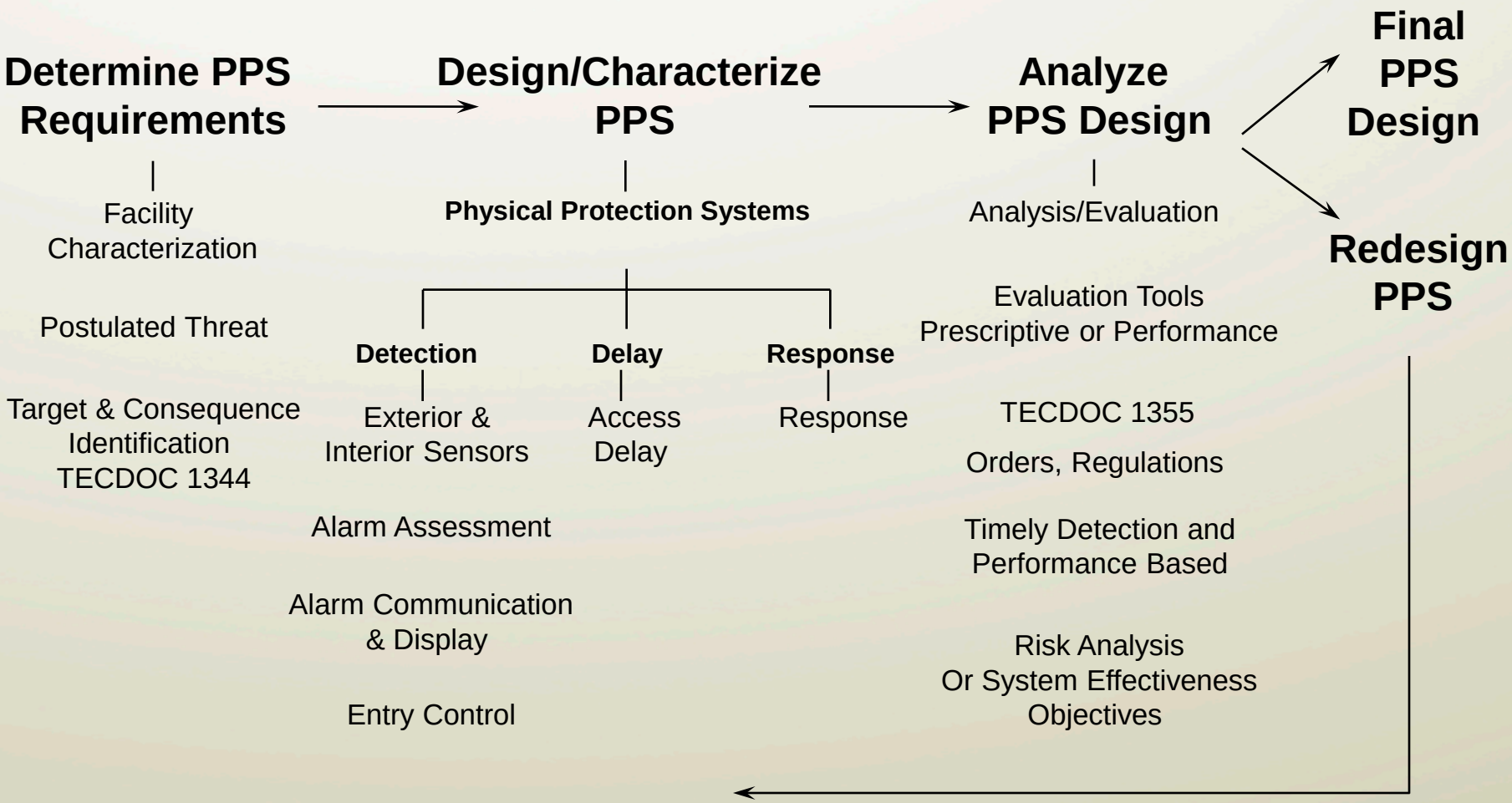
- Appendix II, Table 3 of the Safety Guide describes the potential consequences of each source category (intact and dispersed)
- And the Code of Conduct indicates: "In addition to these categories, States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes."

Source Categorization Summary

- Safety Guide RS-G-1.9 assigns radioactive sources into five categories.
- These categories are used for a variety of purposes, including security.
- Sources are assigned to categories based primarily on their potential to cause harm to human health, as determined by the A/D Ratio.
- States should also take into consideration the potential for sources to cause unacceptable consequences if employed for malicious purposes.

- Physical protection systems
  - Concepts
  - System design

Physical Protection Fundamentals: Design and Evaluation Process Outline



Threat Assessment

- An analysis that documents the credible motivations, intentions, and capabilities of potential adversaries that could cause undesirable consequences by causing sabotage at a facility or stealing a radioactive source

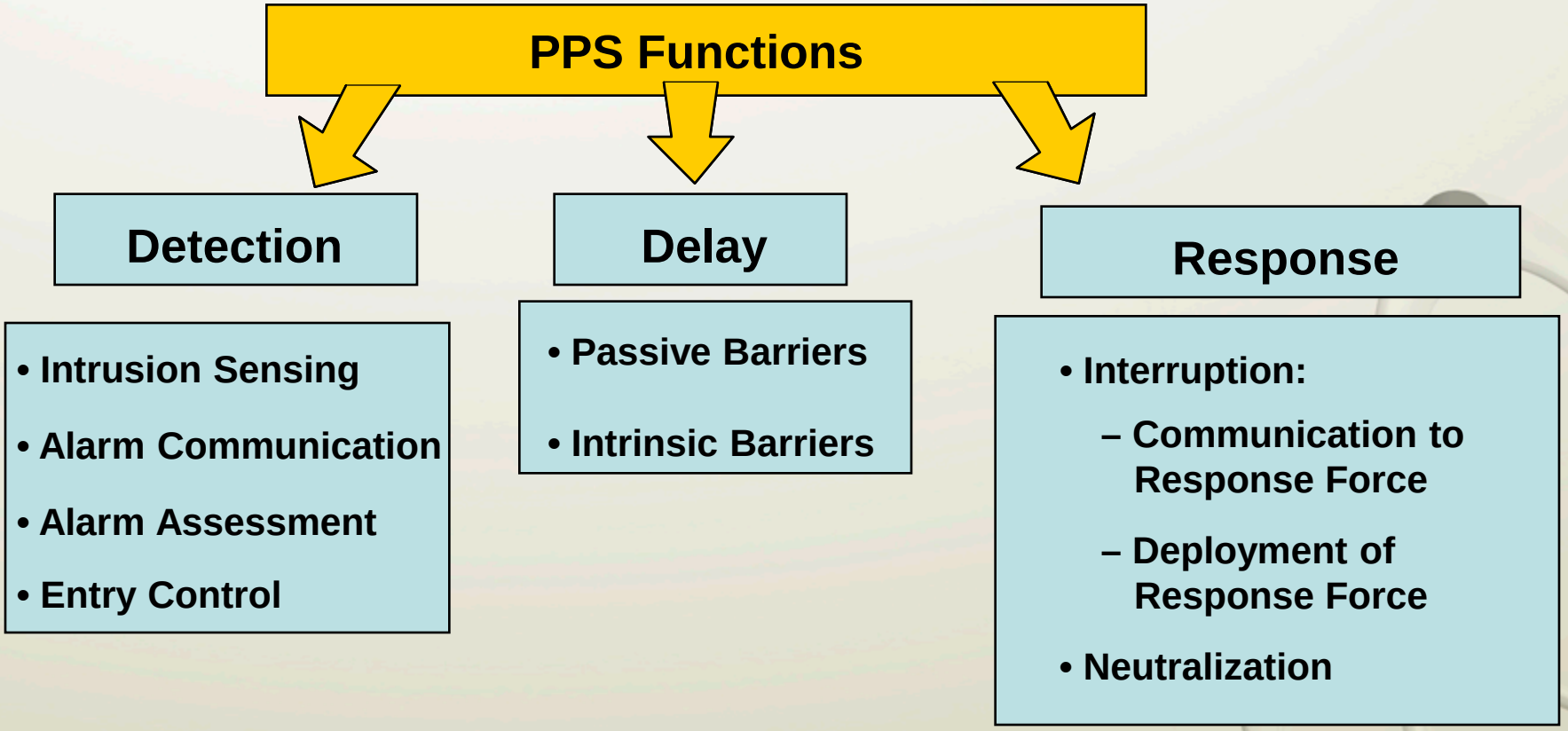
Understanding the Threat

Understanding the Threat

PPS Functions

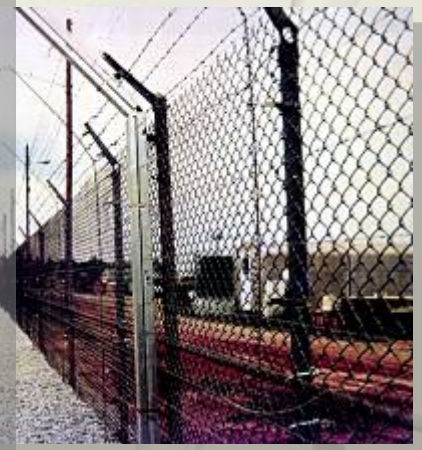
- System functions that must all be present
  - Detection
    - Detects the start of the adversary act
    - Includes the assessment function
  - Delay
    - Retards the adversary to give the response (police or guards) time to respond
    - Effective only after detection is accomplished
  - Response
    - From on-site guards
    - off-site police
    - or military personnel

PPS Functions



Detection

Sensor Activated → **Alarm Signal Initiated** → **Alarm Reported** → **Alarm Assessed**



Delay

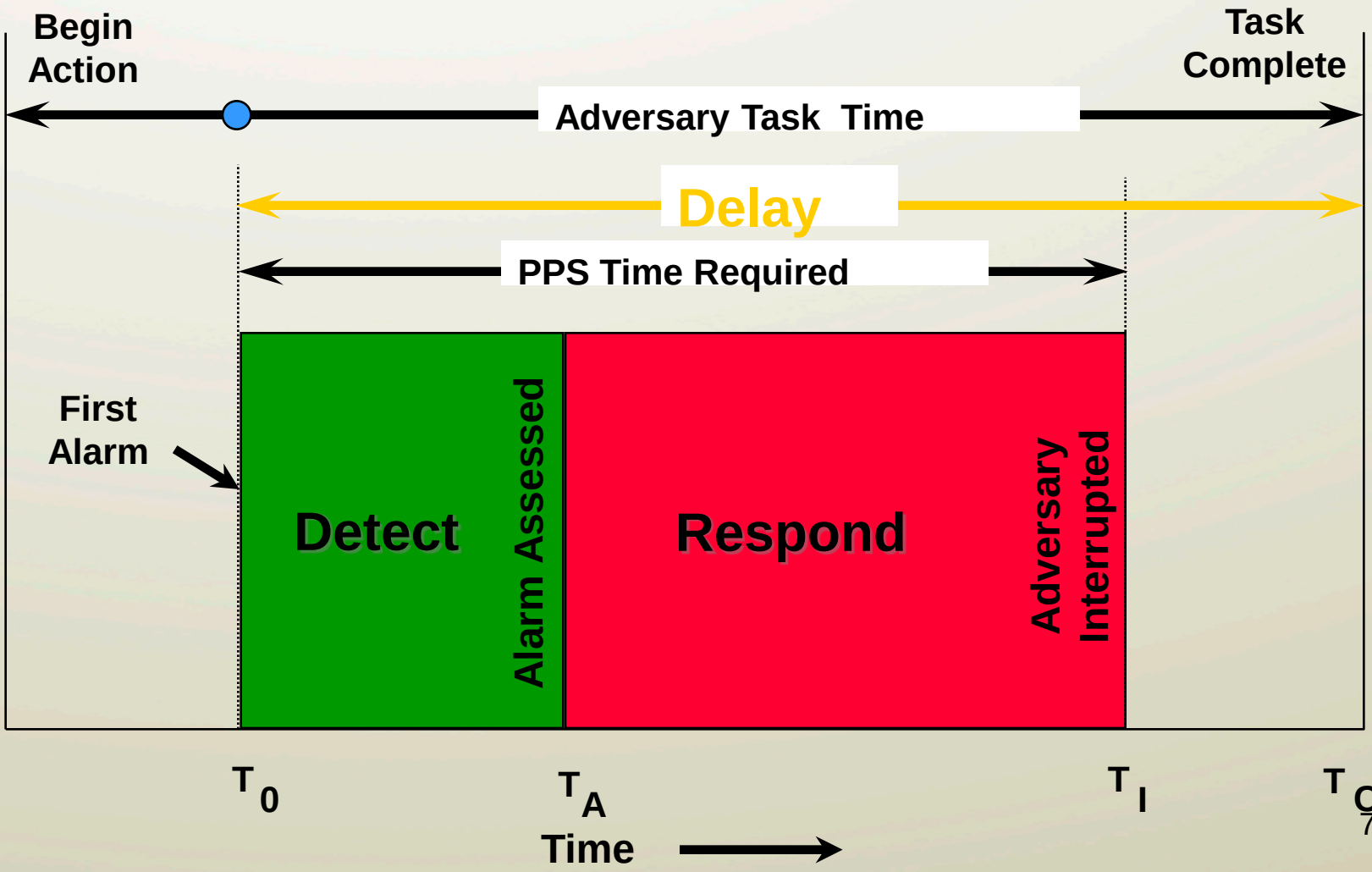
Delay

Provide Obstacles to Increase Adversary Task Time

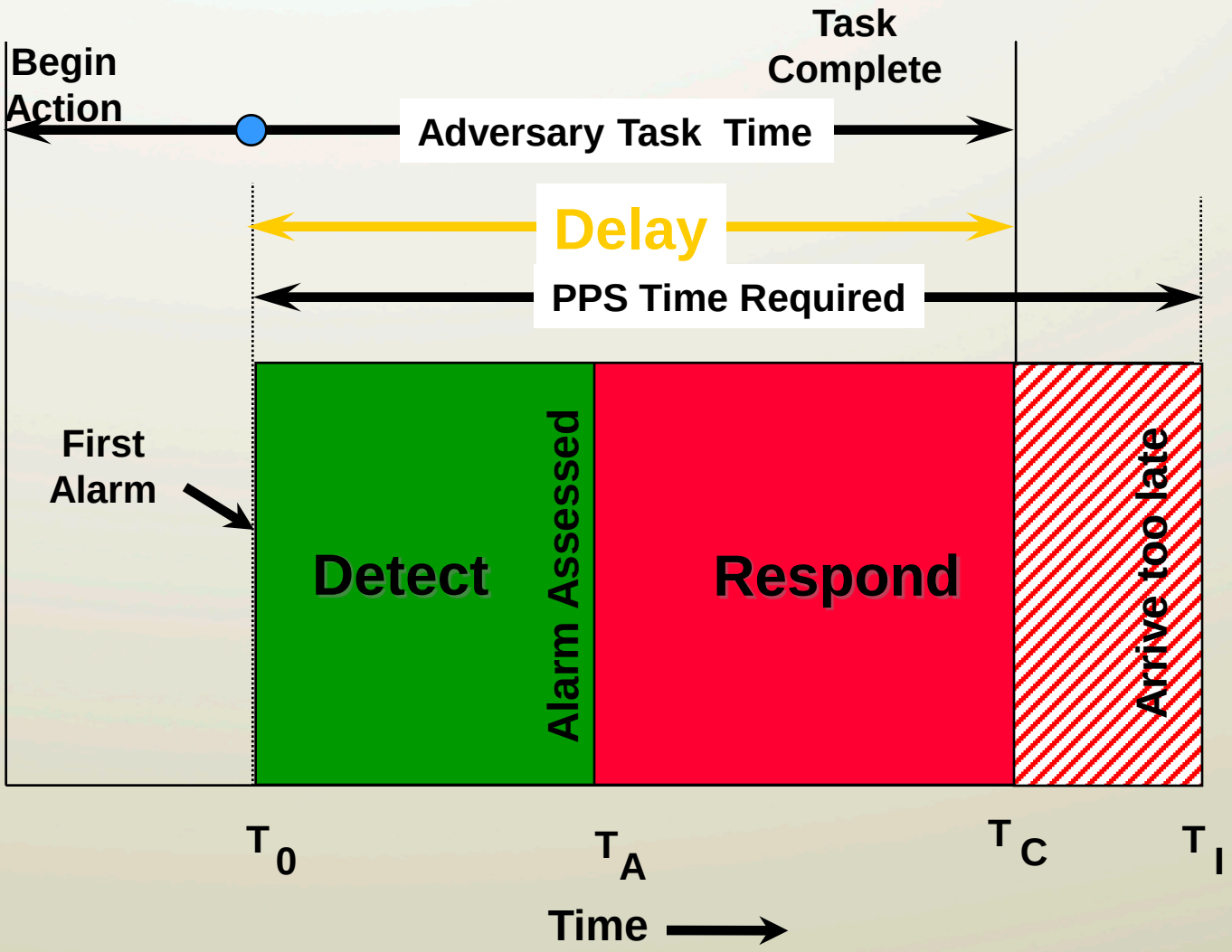
Response

Communicate to Response Force → **Deploy Response Force** → **Neutralize Adversary Attempt**

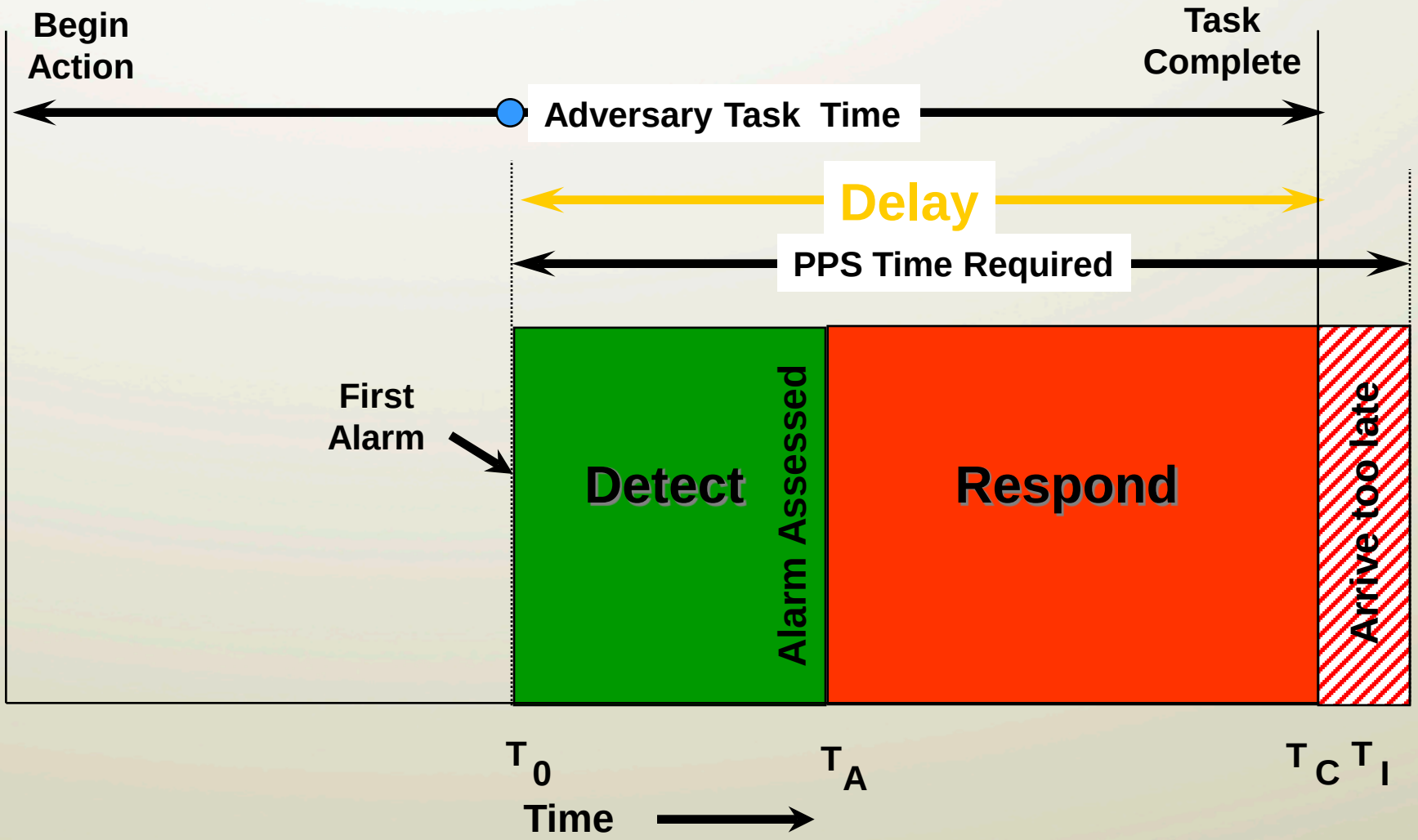
Adversary Task Time vs. PPS Time Requirements



PPS Not Effective (late response)



PPS Not Effective (late detection)



PPS Design Principles

- Place detection toward the perimeter and delay toward the target
- Protection-in-depth
- Minimum consequence of component failure
- Balanced protection
- Combine physical protection components into a system within constraints of the host facility
- Use components that complement each other and correct for weaknesses
- Response able to arrive in time to defeat the threat

Protection-in-Depth

- Adversary must defeat or avoid a number of protective devices in sequence
- Protection-in-depth should:
  - Increase adversary's uncertainty about the system
  - Require more extensive preparations by adversary prior to attacking the system
  - Create additional steps where the adversary may fail or abort his mission

Minimum Consequence of Component Failure

- Contingency plans must be provided so the PPS continues to operate after a component fails
- Redundant equipment can take over function of disabled equipment in some cases
- Some failures require backup assistance from sources external to the facility

Balanced PPS

- Provides adequate protection against all threats along all possible paths
- Conversely, there are no significantly “weak” paths

Sensor Technologies

- Balanced Magnetic Switches
- Vibration and Glass Break Sensors
- Microwave
- Ultrasonic
- Passive Infrared
- Video Motion Detection
- Fiber Optics
- Micro-Switches
- Tamper Switches
- Proximity Sensors
- Weigh Scales

Cameras for Assessment

- Camera on a chip
- Rugged, compact construction
- Evidence-quality
- Very low light cameras
- Infra-red cameras
- LED illumination
- Signal verification
- Pan/tilt/zoom

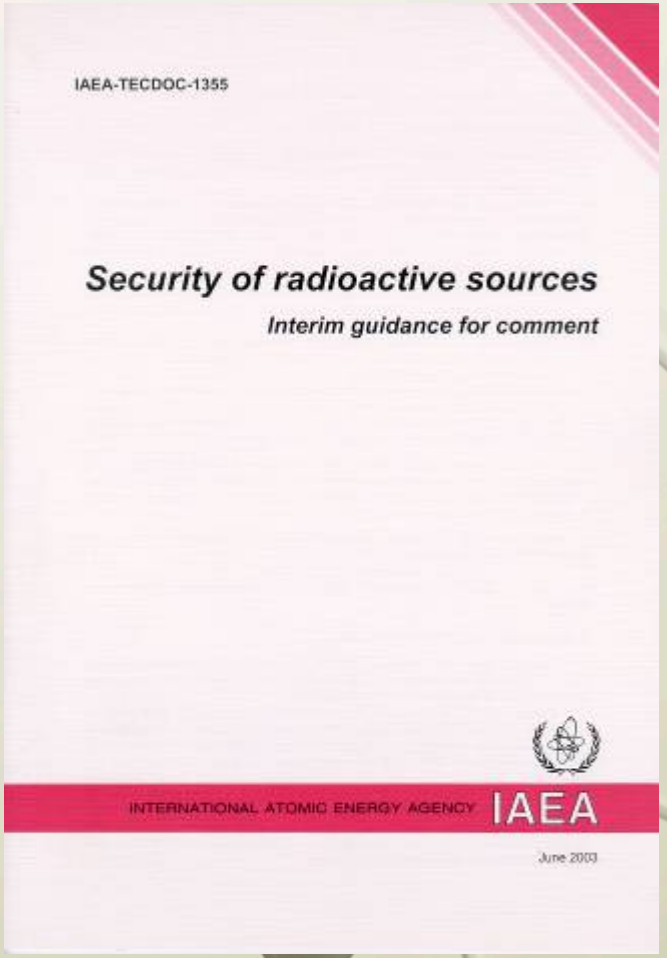
Physical Protection Summary

- Effective physical protection requires:
  - Detection
  - Delay
  - Response
- The total time for detection and response *must* be less than adversary task time once the first detection occurs
- Protection-in-depth, minimum consequence of component failure, and balanced protection are all present in a well-designed system

- Security of Radioactive Sources: TECDOC 1355

TECDOC-1355: Overview

- Primarily addressed to Regulatory Bodies
- Also provides guidance to users
- Assists in identifying security measures consistent with the Code of Conduct
- Recognizes need for balance between managing sources safely and securely while enabling them to be used without undue hindrance
- Premise is that the level of security required should be graded—based on threat, attractiveness, and consequences



TECDOC-1355: Basic Approach

- Design the security program according to a multi-step process
  - Assess the threat of theft or sabotage
  - Determine the attractiveness of sources to adversaries and the potential consequences of theft or sabotage
  - Establish graded performance objectives for security systems
  - Identify a combination of security measures that meets the performance objectives

Assessing the Threat

- Determine “the attributes and characteristics of potential insider and/or external adversaries, who might attempt damage to, or unauthorized removal of, radioactive sources, against which a physical protection system is designed and evaluated”
- Threat assessment can vary widely according to the country, facility, and source
- Can range from very detailed to quite generic

Determining the Attractiveness and Consequences

- Determine the attractiveness of sources to adversaries and the potential consequences of theft or sabotage in either of two ways:
  - Perform detailed assessment, *or*
  - Assign sources to one of four security groups based on the category of the source (TECDOC-1355 Table 2)
    - Each security group corresponds to a different general level of attractiveness/consequences
    - Specific circumstances could justify moving a given source to a higher security group, based on use of the source for malicious purposes (for example, physical form, ease of transport)

Security Groups Based on Categorization TECDOC-1355: Table 2

Security Group	Source Category	Examples of Practice
A	1	Radioisotope thermoelectric generators (RTGs) Irradiators Telegraphy 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 X-ray fluorescence devices Electron capture devices

Establishing the Performance Objectives

- Establish the capability required from security systems on a graded basis
  - as determined by threat assessment and vulnerability analysis, or
  - by assignment of sources to security groups based on the category of the source in Table 2
- Express the required level of capability as performance objectives on the security system
- Performance objectives for the four security groups summarized in TECDOC-1355 Table 1

Performance Objectives
TECDOC-1355: Table 1

<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">Verification of source presence at set intervals</td></tr>
<tr><td colspan="2">Timely detection of unauthorized access</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>

Designing the Security System

- Require the design of security systems to meet the applicable performance objectives through a combination of security measures, including:
  - general administrative measures (common for the management of all sources)
  - administrative measures (graded according to security group)
  - technical measures (graded according to security group)
- Recommended measures for each security group summarized in TECDOC-1355 Table 3

General Administrative Measures

- Security culture
- Emergency plans
- Transfer of sources only to authorized recipients
- Regular source inventories
- Maintenance and updating of source records
- Incident reporting

Administrative Measures

The use of policies, procedures, and practices that direct personnel to manage sources securely and safely

- Access control procedures
- Alarmed access points
- Key control procedures
- Video cameras or personal surveillance
- Inventories
- Reliable and trustworthy personnel
- Information security
- Quality assurance
- Response to an increased threat

Technical Measures

Measures that pose a physical barrier to the source, device, or facility to separate it from unauthorized personnel, and to deter or prevent unauthorized access or removal of a source

- Gates, fences
- Building, walls, roof
- Windows bricked up
- Cages
- Tie-downs
- Locks and interlocks for doors
- Locked, shielded containers
- Intrusion-resistant source holding devices

Recommended Security Measures
TECDOC-1355: Table 3

<table>
<tr><th>Group A</th><th>Group B</th><th>Group C</th><th>Group D</th></tr>
<tr><td colspan="4">General Administrative Measures</td></tr>
<tr><td>Daily Accounting</td><td>Weekly Accounting</td><td>Semi-annual Accounting</td><td>Annual Accounting</td></tr>
<tr><td colspan="2">Access Control to Source Location Allowing Timely Detection of Unauthorized Access</td><td>Access Control to Source Location</td><td rowspan="12">No Specific Provisions. Routine Measures to Ensure Safe Use and Protect as an Asset</td></tr>
<tr><td colspan="3">Deterrence provided by:</td></tr>
<tr><td>Two Technical Measures Separating the Source from Unauthorized Personnel</td><td>Two Measures (one technical) Separating the Source from Unauthorized Personnel</td><td>One Technical Measure Separating the Source from Unauthorized Personnel</td></tr>
<tr><td colspan="2">Specific Emergency Response Plan</td><td>Generic Emergency Response Plan</td></tr>
<tr><td colspan="2">Background Checks</td><td rowspan="8"></td></tr>
<tr><td colspan="2">Security Plan</td></tr>
<tr><td colspan="2">Information Security</td></tr>
<tr><td colspan="2">Upgrade Security for Increased Threat</td></tr>
<tr><td colspan="2">Timely Detection Provided by:</td></tr>
<tr><td>Remotely Monitored Intruder Alarm</td><td>Local Alarm</td></tr>
<tr><td>Timely Response to an Alarm</td><td></td></tr>
</table>

Future Developments

- TECDOC-1355 is being revised as a Security Series guide to include:
  - Elaboration of legislative and regulatory responsibilities, based on the Code of Conduct and other IAEA documents
  - Emphasis on providing guidance to the regulatory body
  - Sharper focus on sources of greatest security concern (Category 1, 2, and 3 sources)
  - Use of terms and concepts consistent with other IAEA security guidance
  - More detailed presentation of security concepts and principles
  - Further explanation of measures and terminology for those without security expertise

TECDOC-1355 Summary

- Primarily addressed to Regulatory Bodies, but also provides guidance to users
- Assists in identifying security measures consistent with the Code of Conduct, through a multi-step process
  - Determine the security risk
  - Establish performance objectives
  - Design the security system
- Revisions to TECDOC-1355 are forthcoming

- Examples of practice-specific Source Security Systems

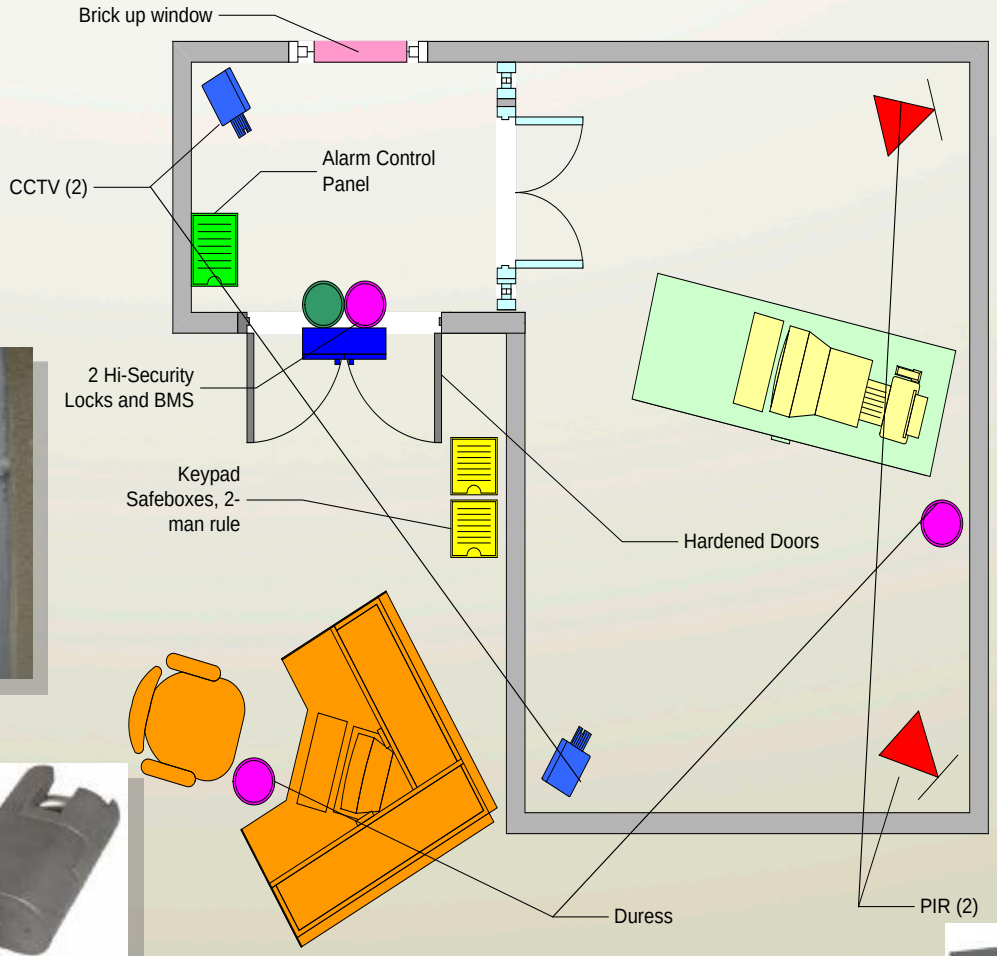
International Cooperation to Secure High-Risk Sources

- Scope:
  - Security for high-risk sources
  - provision of radiation detection equipment
  - Source recovery

Improving Source Security

- Detection
  - Intrusion sensors
  - Video assessment
  - Alarm control and display
- Delay
  - Locks/keys
  - Window gratings
  - Hardened doors
  - Cages
- Response
  - Communications equipment
  - Guard equipment

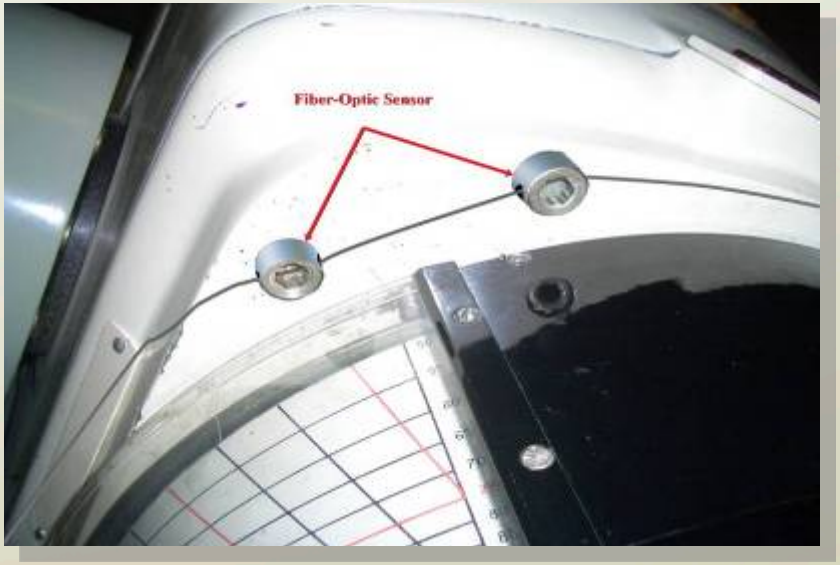
Upgrading Security for Teletheraphy Treatment Room



Upgrading Security for Oncology Clinics

- Improved access control system and intrusion detection sensors to source room
- Low-cost/low-maintenance “always on” sensor to source device

Oncology clinic security enhancements include installation of sensors to detect entry into room that holds source and sensor on the teletherapy unit itself.



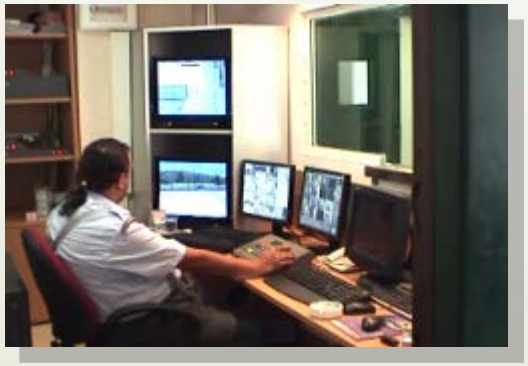
A fiber optic seal encloses the teletherapy unit. Any attempt to access the unit requires breaking the seal, which results in an alarm signal.

Upgrading Security for Self-Contained Irradiators

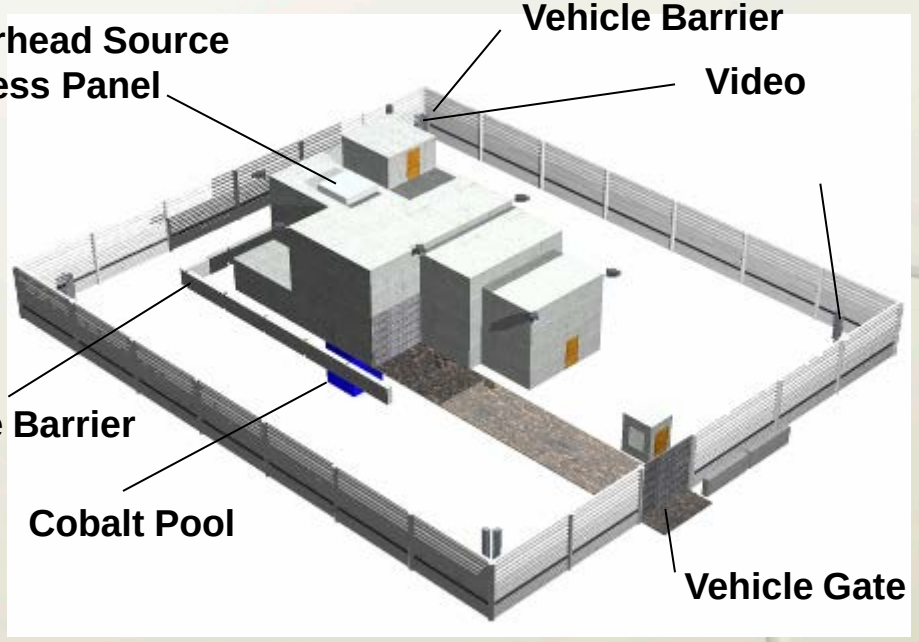
- Delay to prevent source removal:
  - Non-removable screws
  - Welded reinforcements
  - Tie-downs
  - Protecting manuals, etc.
  - Barriers for protection against sabotage
- Manufacturer-provided upgrades

Blood Irradiator Unit. Sensor and fiber optic seal installed on each unit, so an alarm is triggered if an intruder attempts to remove the source.

Upgrading Security for Panoramic Irradiator Facilities (15,000,000 Ci; 555,000TBq)



Alarm Monitoring



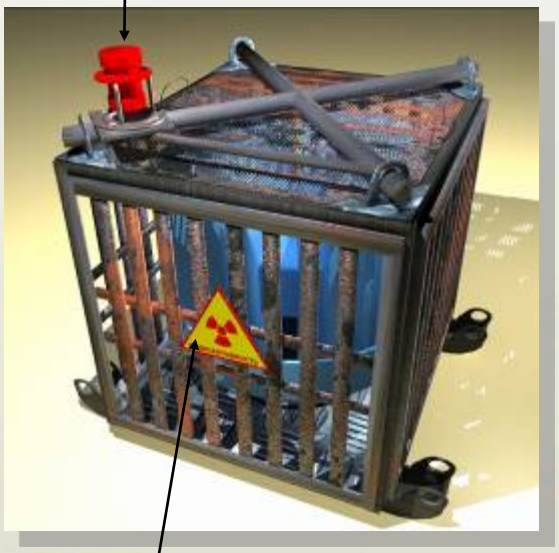
Interior Intrusion Detection

Entry Control

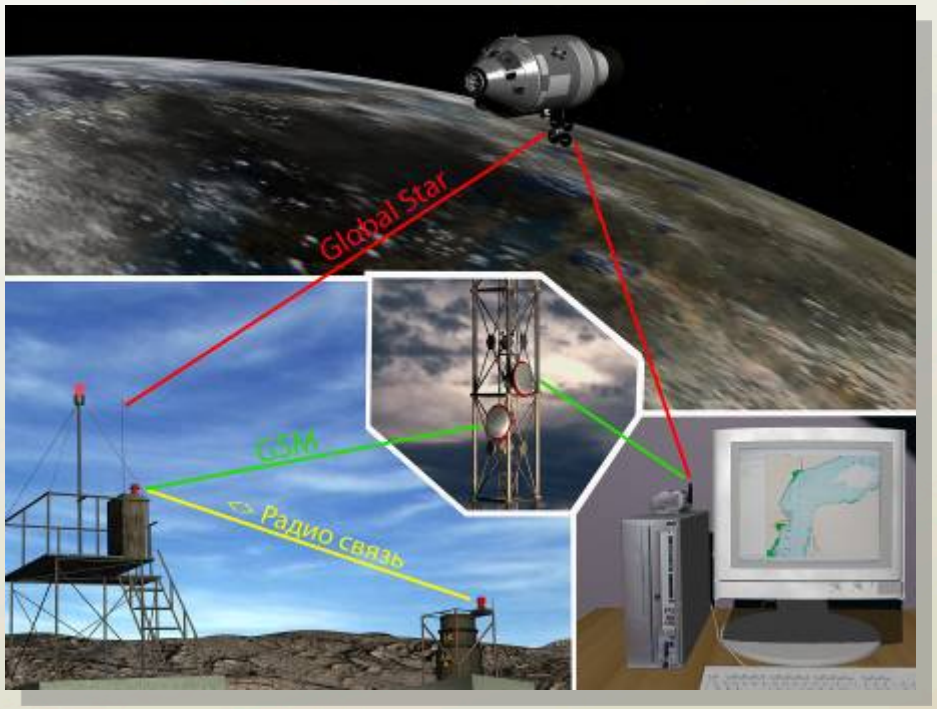
Upgrading Security for Radioisotopic Thermoelectric Generators

(30,000-300,000 Ci; 1,110-11,100 TBq)

- GPS Position
- GSM/UHF Transmitter



- Monitor
  - Vibration
  - Tilt
  - Voltage
  - Temperature



- Remote real-time monitoring of position and status of RTG
- Off-site monitoring through GSM/UHF and satellite communication
- Response dispatched

Discussions

Closing