Guideline

Security of Radioactive Materials

Table of contents

1 Introduction

1.1 Objective and scope of this guideline

'Security' is defined as the complete package of measures that are taken, under the relevant party's own responsibility, to protect an object against harmful influences. These influences can be both external and internal. Security is a way of limiting risks and making them manageable in order to increase safety.

The guideline contains recommendations on securing radioactive materials against theft. This guideline does not substitute any national or international legislation or regulations in this area. Nor does this guideline pretend to replace any multilateral agreements, such as those between cooperating nations within institutes such as the IAEA or EURATOM.

This guideline has been prepared solely for use by radiation protection specialists and should only be used as an aid for effective cooperation with colleagues responsible for security (such as security managers or facility managers). This guideline explains how readers can comply with the Ministerial Regulation on the Security of Radioactive Materials *[MR01].* The Ministerial Regulation on the Security of Radioactive Materials solely applies to the storage and use of artificial radioactive materials and does not apply to activities involving natural sources, activities involving devices or the transport of radioactive materials.

Organisations may opt to secure radioactive materials on the basis of the 'Improved Risk Classification' (IRC) drawn up by the Centre for Crime Prevention and Public Safety (CVV). In this case, the relevant parties must also read the IRC publications[1] 'Security Measures: Definitions' (document D03-385 *[VRKI01]*) and 'Risk Classification for Organisations' (document D03-376 *[VRKI02]*).

1.2 Safety and security

The European Union (EU) and the International Atomic Energy Agency (IAEA) draw up regulations regarding the safety of radioactive materials ('safety') where it concerns their manufacture, use, storage and transport. In the aftermath of "9/11" there has also been increased attention for the security of radioactive materials.

An international convention on the security of nuclear facilities and radioactive materials has been created. Recommendations (IAEA Security Series) and an EU CBRN Action Plan[2] have been drawn up for radioactive materials. The CBRN Action Plan describes the antiterrorism security measures that member states must take. This plan focuses on the misuse of CBRN materials and CBRN resources. The Netherlands has amended its Nuclear Energy Act based on this plan and drawn up recommendations
which have led to two Ministerial Regulations: one concerning the security of nuclear plants and fissionable materials and one concerning the security of radioactive materials.

1Publications can be downloaded from the CCV website
http://www.hetccv.nl/dossiers/Risicoklassenindeling/index?filter=Documentenoverzicht
2CBRN is the abbreviation of **C**hemical, **B**iological, **R**adiological and **N**uclear.

This guideline concerns the ‘security’ of radioactive materials and will only refer to ‘safety’ where this is needed to explain a particular theme.

2 Importance of security

Radioactive materials can harm humans and/or the environment as a result of errors in their manufacture, incorrect use, incorrect storage or poorly organised transport. The nature of the situation in which unintentional exposure occurs determines the severity of the damage. Safety recommendations and guidelines have been drawn up for the use of radioactive materials at both the national and international levels. The focus of these recommendations and guidelines is ‘safety’.

A few of these recommendations and guidelines also discuss aspects of ‘security’, such as the ‘International Basic Safety Standards for Radiation Protection and Safety of Radiation Sources’ *[IAEA01].* In this document, the IAEA writes, for example:

- *Security is defined as the prevention and detection* of, *and response to theft, sabotage,*
  unauthorized access, illegal transfer or other malicious acts involving radioactive material…
- *There is not an exact distinction between the general terms safety and security. In general, security is concerned with malicious or negligent actions by humans that could cause or threaten harm to other humans; safety is concerned with the broader issue of harm to humans (or the environment) from radiation, whatever the cause. The precise interaction between security and safety depends on the context*
- *Safety measures and security measures have in common the aim of protecting human life and health and the environment. In addition, safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.*
- *Security infrastructure and safety infrastructure need to be developed, as far as possible, in a well coordinated manner. All organizations involved need to be made aware of the commonalities and the differences between safety and security so as to be able to factor both into development plans. The synergies between safety and security have to be developed so that safety and security complement and enhance one another.*

At the European level, general regulations on the protection of humans, plants, animals and goods against the harmful effects of exposure to ionising radiation are recorded in EU Directive 96/29 *[EU01].* This Directive prescribes a system of licences that are linked to standards. This system has since been implemented in Dutch legislation. In Art. 14 of the Radiation Protection Decree it is prescribed that radioactive materials must be secured against theft and damage and against unauthorised use with malicious intent (general duty of care for organisations) *[BS].*
The increased threat of terrorist attacks since “9/11” has led to an increased focus on the theft and misuse of radioactive materials. For example, the IAEA has amended the ‘Code of Conduct on the Safety and Security of Radioactive Sources’ and tightened its security principles*[IAEA02].* At the European level, initiatives have been launched to improve protection against terrorist threats to CBRN resources. The European Ministers of Justice and Internal Affairs have agreed to a European Commission *action plan [EU02].* This plan describes a cohesive approach at the European level to reduce the likelihood of an attack or

accident involving CBRN materials or resources. Although the likelihood of an attack is small, if such an attack should take place the consequences could be enormous.

Due to these developments, it was decided that further elaboration of the general duty of care, as described in Art. 14 of the Radiation Protection Decree, was needed in the form of a Ministerial Regulation with a more concrete description of said duties. The Ministerial Regulation on the Security of Radioactive Materials focuses mainly on preventing and limiting the likelihood of 'theft', the thinking behind this being that the likelihood of misuse can be limited considerably if sufficient security conditions are met. The underlying principle is that if adequate measures are taken against theft, said measures will also prevent misuse. The regulation does not describe specific antiterrorism measures and facilities. Such measures and facilities are described on the website of the National Coordinator for Security and Counterterrorism (NCTV)[3].

The Nuclear Energy Act and the Radiation Protection Decree together form the foundation of the Ministerial Regulation on the Security of Radioactive Materials. The Nuclear Energy Act is a framework act which describes the authority of the national government, opportunities for additional legislation and a system of licences. The main objective of this Act is the protection of the environment, employees and the public against the harmful effects of ionising radiation. Various administrative orders (AMvB or decree) and Ministerial Regulations (MR or regulation) are linked to the Act which describe how regulations for working with sources of ionising radiation must be implemented. An important decree that effects radioactive materials is the Radiation Protection Decree. This decree describes the basic rules for working with sources of ionising radiation (encapsulated sources, open radioactive materials and devices), such as:

1. the basic principles for radiation protection (justification, ALARA principle and dose limits);
2. general rules on expertise and training;
3. specific rules for the protection of the public, employees and patients against the harmful effects of exposure to ionising radiation;
4. further elaboration of the system of licenses.

Other relevant decrees in relation to the Nuclear Energy Act are the High-Activity Sources Decree and the Fissionable Materials, Ores and Radioactive Substances (Transport) Decree. An up-to-date overview of legislation and regulations can be found on the website of NL Agency[4].

3 http://www.nctv.nl
4 http://www.agentschapnl.nl/programmas-regelingen/stralingsbescherming-wet-en-regelgeving

3 Security and security methodology

3.1 General

Due to various events and the changing needs of society, the idea of ‘security’ has gone through major developments since the beginning of this century. Sites and objects that need securing can vary widely. For example, there are differences in the ways that radioactive materials are manufactured, stored, used and transferred. The conditions under which radioactive materials are applied differ too, for example in hospital settings (open sources for nuclear medicine) or industrial settings (closed sources for measurement and control technology). These materials may also be used in different ways within a single application, such as in permanent measuring equipment or in varying locations. There are countless other examples among the hundreds of licensees registered with NL Agency. It is therefore logical that these differences lead to variations in how security measures and facilities are implemented.

However, there are also similarities, the most important of which is the approach to security. Regardless of the situation, the security of radioactive materials can always be arranged by setting up and maintaining a ‘security management system’ (SMS). This professional and systematic approach to risk management is described in detail below. Alongside the SMS, other management systems may also be operational, for example with regard to quality or safety.

3.2 ***Security plan***

In order to implement security measures and facilities cost-effectively, the security of an organisation must be methodically and systematically organised. This approach results in the description of a security management system (SMS). In order to establish an SMS, a security policy must be formulated, a risk identification and analysis must be performed, the security organisation must be established and security measures and facilities must be put in place. A comprehensive SMS will provide the organisation with insight into the effectiveness and efficiency of the existing and yet to be established security measures and facilities.

The Ministerial Regulation on the Security of Radioactive Materials provides only a limited description of such a system. The results of the SMS must be summarised in a security plan. Security plans will differ between various organisations. A security plan is important because it forms the foundation of the security measures that are required to secure radioactive materials against theft or misuse. The security measures that are adopted must guarantee the detection of attempted theft and misuse and that such an attempt will result in the immediate activation of a hold-up time before persons with malicious intent can access the radioactive material.
An SMS is typically established in large organisations, who hire or employ specific security personnel for this task. The establishment of an SMS may be too complicated or large a task for smaller organisations. Moreover, because the Ministerial Regulation on the Security of Radioactive Materials prescribes only protection against ‘theft or misuse’, it is not always necessary to establish an SMS. This pragmatic approach enables smaller organisations, where there are no major risks due to the nature of the applications, to opt for a security system based on the CCV’s Improved Risk Classification (IRC). This instrument is part of the

CCV's BORG certification scheme[5] and offers a practical guide to meeting the requirements of the scheme. Organisations are permitted to establish alternative security systems on condition that the same end result is intended. This guideline does not discuss this option further.

3.3 Improved Risk Classification (IRC)

The IRC is an instrument for determining the security risk of, among others, business premises using risk categories and for determining which combination of security measures is most suited to limiting this risk. The application of the IRC gives organisations insight into their own security. The quality of their security can be confirmed by means of a BORG security certificate. Owners of premises can use the certificate to demonstrate to insurers that they have installed a suitable security system. The IRC instrument that is part of the BORG certification scheme was created in collaboration with security industry specialists, insured parties and their insurers and is administered by the CCV.

The BORG security certificate provides assurance on the quality of the security measures and the manner in which they have been applied, but its primary function is to assure the cohesiveness of these measures and their capacity to secure the relevant premises. A BORG security certificate is only issued if all security measures (or equivalent, made-to-measure solutions) required for a particular security category have been implemented.

The IRC is described in various publications. We advise using the publication 'Security Measures: Definitions' and the IRC chart *[VRKI03]* alongside this guideline. These describe and explain the various security measures required in accordance with the risk classification system for securing a home or organisation against intruders. The security measures are described (see further on in this document) as well as the required level of implementation for various risk categories. In some cases, alternative security measures can be adopted, as these can result in better solutions than the prescribed measures. These are described as 'equivalent measures'.

For a general understanding of the subject matter, it may be necessary to read the publication entitled 'Risk classification for organisations'. This publication describes how organisations can 'measure' the risk of a break-in and 'implement' the most suitable theft prevention measures. Other CCV publications are less relevant to the security of radioactive materials.

3.4 Offender profiles

The IRC is based on an analysis of a large number of recorded intrusions of business premises. The analysis is based on a number of offender profiles that have been derived from the general threat assessment. Under normal conditions, this general threat assessment describes the most likely threat to an organisation, in other words, the risk of becoming the victim of theft or misuse. The analysis has produced characteristics of the type of offender, offenders' methods and the equipment used by offenders. This set of characteristics is called the offender profile.

The offender profile reflects the current knowledge on real and potential offenders and covers situations in which offenders have the intention to enter and/or approach the premises of a

5 For an explanation of the BORG certification scheme, see *[VRKI01],* item 1.2

business, organisation or home with the intention of influencing or disrupting a process or the privacy of the owner without authorisation. Alongside criminal intent, the motives may also be political or religious in nature. The following offender profiles are distinguished under normal conditions, i.e. if there is no threat of terrorism:

- Errant youth, whose normal play develops into errant behaviour. The theft of goods is usually not the immediate goal.
- Amateur or opportunist offenders, who commit a crime because the opportunity or situation presents itself and there is a low risk of being caught.
- Semi-professional or regular criminals, whose income partly or wholly consists of the proceeds of crime as well as those who are forced to steal due to circumstances. This category of offender takes more risks.
- Professional criminals, whose income usually wholly consists of the proceeds of criminal activities. The difference between professional and semi-professional criminals is mainly in the degree of specialisation in the preparation and execution of a crime.
- Terrorists, who commit crimes for ideological reasons. Terrorists focus on preparing and committing serious violent crime. The intention is usually to disrupt society with the aim of forcing social change, terrorising the population or influencing political decision-making.

The first two offender profiles are the most common. The offender profile defines the standard for the implementation of security measures. It is an assessment criterion for determining the effectiveness of the security measures and facilities. After all, these measures and facilities must be sufficient to stop those categories of offenders that are most likely to form a risk.

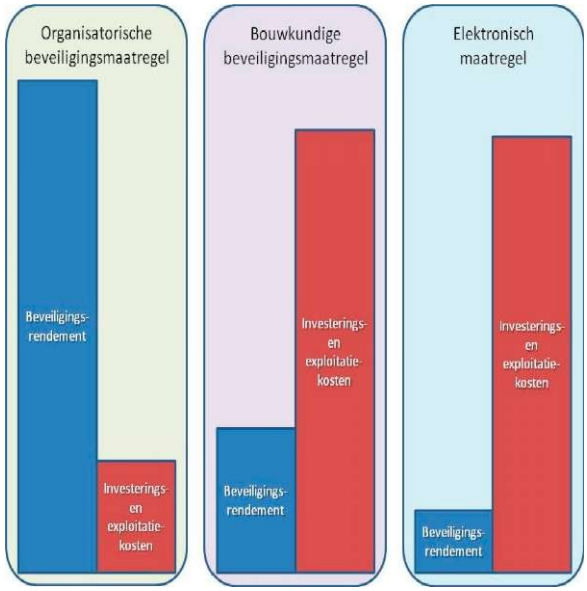
Intrusions resulting in theft can be executed by both external and internal offenders, or a combination of both. Internal offenders may be represented in various offender profiles. The risk of internal offenders can be limited by means of pre-employment screening (verifying a person’s data before he or she is employed) and adequate internal security (procedures, compartmentalisation, authorisations, etc.). External offenders may attempt to acquire information or resources that they can use to commit a crime by influencing employees. In order to limit this risk, the Ministerial Regulation on the Security of Radioactive Materials prescribes that organisations must require employees who are familiar with the organisation’s security plan to present a Certificate of Good Conduct.
The National Coordinator for Security and Counterterrorism (NCTV) and/or the General Intelligence and Security Service (AIVD) regularly perform threat analyses. The current threat level is updated daily on the NCTV’s website.

3.5 Security measures

We are regularly confronted with security measures in daily life, for example when we wish to enter a certain building (reporting to the reception, displaying an ID card, using a visitor pass) or at airports (luggage inspections).

Security measures differ in their nature. Most security measures are organisational measures (O). These include procedures, agreements, etc. A bomb alert procedure is an example of an organisational measure. Access to a building via a turnstile gate is a physical measure (P). Security cameras, passive infrared detectors and systems that alert a commercial emergency call centre are electronic measures (E).

Security measures are interconnected; one measure backs up another with the aim of creating cohesive security. A sufficiently cohesive security system can be designed by implementing an effective combination of O, S and E measures (OSE mix). The IRC helps organisations to choose the best OSE mix for their specific situation (this is discussed later in this guide).



The effectiveness of this
mix of security measures is determined by the answer to the following question: ‘Are we capable of managing unwanted incidents?’ The efficiency is determined based on the investments and the operational costs of the measures in relation to the material and

immaterial value of the interest to be protected and the effectiveness of the measures taken. Generally, organisational measures entail the least investment and the lowest operational costs while their yield and/or effect is greater in comparison with physical and electronic measures. Physical and electronic measures generally entail the largest investment and the highest operational costs while their yield is relatively low in comparison with organisational measures.

This background information makes it possible to come to an optimum mix of organisational, physical and electronic measures in order to achieve the security objective.

3.6 Risk and security categories

The IRC makes use of a number of risk and security categories. Each risk category is linked to a security category that entails the most suitable combination of security measures. The IRC describes one or more combinations of security measures for each security category. These mixes of measures together form the most suitable combinations of security measures.

The document 'Security Measures: Definitions' describes the possible security measures in detail. These measures are symbolised by the following letters: **O**rganisational, **P**hysical (**U**nauthorised removal prevention/**C**ompartmentalisation), **E**lectronic, **A**larm systems and Response. The measures can be specified further using codes, such as O1, O2, etc. This enables the complete package of security measures to be displayed using a limited number of letters and numbers.

For example, the following letter/number combinations are used for displaying the security measures:

- O1, O2 organisational measures
- P0, P1, P2, P3 physical measures
- E1, E2, E3 electronic measures
- C/U1, C/U2, C/U3 compartmentalisation/unauthorised removal prevention measures
- A1, A2, A3, AoIP alarm systems
- R1, R2, R3 response (alarm response)

The IRC chart provides a convenient overview of the definitions of the various measures.

If the security has been organised according to a certain security category then a BORG security certificate can be requested from a BORG certified security company. If the security measures meet the requirements then the BORG certified security company is required to issue the certificate.

3.7 Timeline analysis and security yield

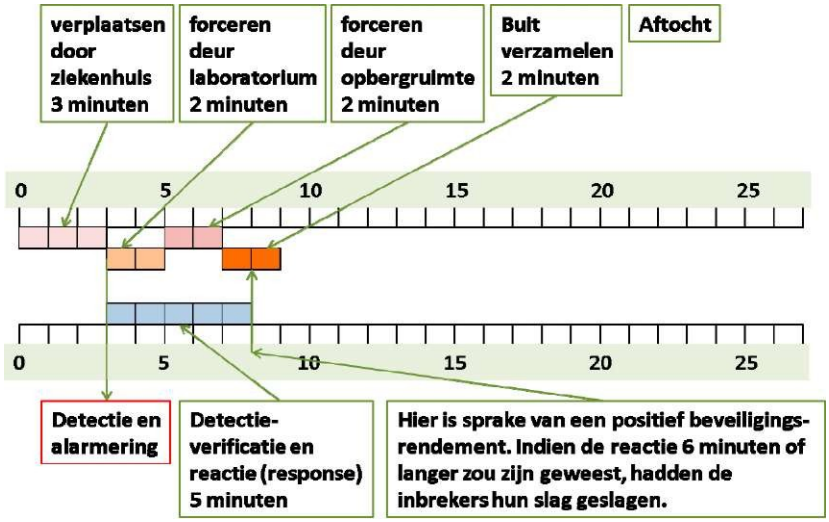
An organisation can determine if the security is in order by performing a timeline analysis (PICE/ALRE). First the possible actions of the offenders are depicted on a timeline (PICE: Planning, Intrusion, Collection of property, Escape). Then the same is done for the security measures and facilities that are in place by calculating the movement times and hold-up times (ALRE: Alarm and Response). The two timelines are then compared.

The following case study illustrates how this works and clarifies a number of matters. The case study concerns a theft from a hospital laboratory.

An offender has targeted a number of goods in a hospital laboratory. To gain entry to the laboratory, he must first make his way through the hospital.
He then needs to force the door to the laboratory, followed by the door to the storage cupboard. He now has access to the goods, which he takes and then makes his getaway. These actions take him a total of 9 minutes.

A detector is activated as soon as he forces the first door. The time between this alarm and the offender starting to make his getaway is the hold-up time. The detector generates an alarm at the security desk located at the hospital entrance. One of the security guards goes to the location to check on the situation. When he sees it is a real alarm (i.e. not a ‘false alarm’), he alerts the police via the security desk. After receiving the alert the police immediately go to the hospital (it is classified as an urgent call if the hospital is registered as a CBRN business) and try to arrest the offender (in the act).

If the theft is prevented then this was a case of a positive security yield and/or there was sufficient security in place. If the theft is not prevented then this was a case of a negative security yield and/or there was insufficient security in place.



4. Security of radioactive materials

4.1 Objective of the Ministerial Regulation on the Security of Radioactive Materials

The Ministerial Regulation on the Security of Radioactive Materials describes who is responsible for securing radioactive materials and at which level of implementation this must be done. The security measures taken on the basis of this Regulation must secure the radioactive materials against theft or misuse as much as is reasonably possible. The security

in place prevents third parties from taking radioactive materials where this is ‘unauthorised’, ‘unintended’ or ‘unwanted’.

In assessing the risks, there are various situations that can take place throughout the logistical chain:

a. transport;
b. situations where transport is temporarily interrupted, such as when parking;
c. storage of radioactive materials during or in connection with transport;
d. fixed (permanent) locations (use and storage);
e. temporary locations where radioactive substances are used.

The security regulations for transport (under a, b, and c) are described in the ADR/VLG[6]. This guideline does not discuss these regulations further. This guideline does define and explain the security measures required by the IRC method for the prevention of theft where it concerns the use and storage of radioactive materials (under d and e).

4.2 Security categorisations of radioactive materials

The Ministerial Regulation on the Security of Radioactive Materials applies to licensees who are licensed to perform activities with radioactive materials (Art. 24 and 25 of the Radiation Protection Decree). The Regulation solely applies to the storage and use of artificial radioactive materials. The Regulation does not apply to activities with natural sources, activities with devices and the transport of radioactive materials.

The radioactive materials to which the stipulations in the Regulation apply have been divided into a number of categories. These categories follow the recommendations in the IAEA document ‘TECDOC-1344’ *[IAEA03].* This document describes a system in which artificial radioactive materials are categorised on the basis of risk. Five risk categories are distinguished in the IAEA recommendations, as described in Nuclear Security Series No. 11 *[IAEA04].*

These risk categories correspond to the security objectives (which are also described in the IAEA recommendations):

- Category 1: Security level A, prevent unauthorized removal of a source.
- Category 2: Security level B, minimize the likelihood of unauthorized removal of a source.
- Category 3: Security level C, reduce the likelihood of unauthorized removal of a source.
- Category 4 & 5: Follow Basic Safety Standards.

The Ministerial Regulation on the Security of Radioactive Materials covers only the first three risk categories in the IAEA recommendations. It was concluded that the last two security categories are sufficiently covered by the ‘due care’ stipulation in Art. 14 of the Radiation Protection Decree. Based on the security objectives, this means that the security measures for the category 1 materials described in the Regulation must result in

6 ADR is the abbreviation of the French title of the European Convention concerning the International Carriage of Dangerous Goods by Road: “Accord européen relatif au transport international des marchandises Dangereuses par Route”. The text of this convention has been translated into Dutch and can be found in Annex 1 of the Regulations on the Carriage of Dangerous Goods by Road (VLG). The supplemental and deviant regulations for the territory of the Netherlands are described in Annex 2 of the VLG.

the actual prevention of theft of these materials. With regard to category 2 materials, the security measures must minimise the likelihood of unauthorised removal. With regard to category 3 materials, the security measures must reduce the likelihood of unauthorised removal. In the Regulation, the IAEA objectives are translated into specific requirements for detection and hold-up times per category.

There are a number of differences in the definitions used and in the division into categories. *Table 1* is a comparative overview of the IAEA categorisation of radioactive substances with the corresponding security levels and the risk and security categories used in the IRC.

Security categorisation (according to Table 5 of the IAEA Nuclear Security Series No. 11, Implementing Guide, Security of Radioactive Sources - page 23)	IRC Risk category	**Security level** (according to Table 5 of the IAEA Nuclear Security Series No. 11, Implementing Guide, Security of Radioactive Sources - page 23)	IRC Security category
1	4	A	4
2	3	P	3
3	2	C	2
4	1	Basic Safety	1
5		Standards	

Table 1 Comparison of the security categories and security levels of the IAEA and the IRC

The IRC division into risk categories ranges from 4 (major risk) to 1 (low risk). This corresponds with the division into security categories, which likewise range from 4 (heavy security) to 1 (light security). A larger risk implies heavier security.
Table 2 displays the division into security categories of commonly used radioactive materials in relation to the IAEA category, the IAEA security levels, the IRC risk categories and the IRC security categories.[7] This categorisation takes into account the desirability of these materials, simply because some radioactive materials are easier to appropriate (and therefore more desirable) than others. The starting point is: “The greater the desirability, the higher the risk category.” These materials are specifically described in the third column of Table 2.

The third column also lists the criteria for A/D values. A stands for the Activity as meant in Art. 1 of the Radiation Protection Decree. The D (Dangerous) value, which describes the

7 This table is from the Ministerial Regulation on the Security of Radioactive Materials. The table is based on IAEA Nuclear Security Series No. 11, Implementing Guide, Security of Radioactive Sources; TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES, modified.

level of danger of the applicable nuclide, is determined using Table 1 of the IAEA document ‘EPR-D-Values 2006’, using lowest value *[IAEA05].* The risk category (and thus the corresponding security category) of applications that are not explicitly described in the table can be found by calculating the A/D value of the material and comparing the result with the A/D values in the table. Radioactive materials that are not explicitly categorised are categorised on the basis of the A/D value.

If there are several radioactive materials in a space that are not secured separately, then the sum of the A/D values is used:

$$A/D = \sum_{n} \frac{\sum_{i} A_{i,n}}{D_n}$$

where:
A_{in} = activity (in Bq) of each radioactive material or encapsulated source i with radionuclide n D_n = D value (in Bq) for radionuclide n

For the categorisation, the total activity of the sources and nuclides in a single space must considered as a whole. It should be clear that if several materials are stored in a space, the minimum security level will be determined by the highest risk category.

With regard to all other radioactive materials, including those described in IAEA categories 4 and 5, the stipulations in the Radiation Protection Decree and the license regulations describe specific regulations on radiation safety that simultaneously provide sufficient protection with regard to the security of radioactive materials.

IAEA category/ MR category	IRC Risk category	Radioactive materials:	IAEA security level	Security category
1	4	Artificial radioactive materials for: - nuclear batteries, - sterilisation, examination and blood irradiation, - teletherapy equipment, - fixed multi-beam teletherapy Or Other artificial radioactive materials of which: A/D >1000	A	4
2	3	Artificial radioactive materials for: - industrial gammagraphy, - brachytherapy (absorbed dose of 2.0 Gy or higher) Or Other artificial radioactive materials of which: 1000 > A/D > 10	P	3
3	2	Artificial radioactive materials for: - high-activity sources with radioactive materials in permanent industrial measurement equipment, - well measurement equipment for oil and gas extraction (well logging) Or Other artificial radioactive materials of which: 10 > A/D > 1	C	2

Table 2: Categorisation of radioactive materials

IAEA Category	Risk category IRC	Security level IAEA	IRC security category	Security measures for fixed (permanent) locations					Security measures for non-permanent locations
4 and 5	1	Basic Safety Standards	1	**O**	**P**	**E**	**R**	**Comments**	During the activities: the security requirements in accordance with corresponding risk category
				O1	P1			-	
				O1	P0	E1	R1	-	
3	2	C	2	**O**	**P**	**E**	**R**	**Comments**	
				O1	P1	E1	R1	-	
				O1	P1 +C/U1	E1	R1	-	
				O1	P0 +C/U2	E2	R1	-	
2	3	P	3	**O**	**P**	**E**	**R**	**Comments**	
				O2	P2	E2	R2	1	
				O2	P3	E2	R2	1	
				O2	P2+C/U2	E2	R1	-	
				O2	P0+C/U3	E2	R1	-	
1	4	A	4	**O**	**P**	**E**	**R**	**Comments**	
				O2	P3	E3	R3	1+2	
				O2	P2 + C/U2	E3	R3	1	
				O2	P1 + C/U3	E3	R3	-	
Comments	1. Perimeter detection level 2 2. Perimeter detection near storage area level 3 The term ‘perimeter detection’ is used rather than ‘facade detection’ because the perimeter of, for example, a storage area can also be a wall adjoining an adjacent company or office space. Perimeter detection involves intruder detection outside the perimeter wall, as also applies to the term C/U: “raise the alarm first and only then activate hold-up measures”.								
Alarm transmission	Category 2: A 1 alarm transmission system A 2 alarm transmission system A 3 alarm transmission system Category 3: Category 4:								

Table 3 Possible security measures for different risk categories[8]

4.3 Security categories and determination of security measures

The translation of the IAEA recommendations into IRC categories, as described in Table 1, makes it relatively easy to determine the right security measures for a certain radioactive material category. Table 3 *displays the relationships between the IAEA categories, the IRC risk categories, the IAEA security levels, the IRC security categories and the security measures.*

8Terms such as ‘perimeter detection’ are also explained in the IRC document ‘Security Measures: Definitions’.

4.4 Security plan

A security plan that describes the current situation is compulsory for the security of category 1, 2 and 3 radioactive materials. The security plan shall contain at least:

a. Name and description of the property or site (or part thereof) to be secured.
b. The security objective, including:
   - a description of the radioactive materials to be secured;
   - a description of the manner and location of storage and use of the radioactive materials;
   - the radioactive material categories;
   - a description of the measures to be taken in accordance with the security category corresponding to the relevant risk category.
c. If a BORG security certificate is to be requested: determine whether the security must be organised
   on the basis of a security system (involving the issue of a BORG security certificate) or on the basis of a BORG Operational Certificate.
   - If the objective is a security system, then the security plan will provide a specification of the security measures to be taken, including a timeline analysis. In case of small properties, an indication will suffice in place of a timeline analysis.
   - If the objective is a 'BORG Operational Alarm System Certificate' for the electronic measures, then the security plan will provide a specification of the electronic and response measures (E and R), as well as the corresponding organisational measures (O), including the timeline analysis of the alarm system. In case of small properties, an indication will suffice in place of a timeline analysis.
   - If the objective is a 'BORG Operational Physical Security Certificate', then the security plan shall provide a specification of physical (P) and, if applicable, compartmentalisation/unauthorised removal prevention (C/U), measures as well as the corresponding organisational (O) measures.
d. Organisational measures[9] (O):
   - general;
   - specific.
e. Physical measures (P):
   - additional physical measures (if applicable);
   - unauthorised removal prevention measures (U);
   - compartmentalisation (C, if applicable). f. Electronic measures:
   - Intruder Alarm System (A);
   - service and maintenance contract;
   - if applicable, the connection to and contract with a commercial emergency call centre;
   - agreements with key holders and/or commercial security organisations;
   - agreements with commercial security services and the police, fire service and/or ambulance services (regional medical assistance command structure (GHOR)) on both internal and external measures in case of a security incident. This includes informing the police that the organisation is registered as a CBRN business.

The security measures will be described as much as possible in the form of performance requirements set down in a schedule of requirements. In other words, it is not described

9 A complete description of the organisational and technical security measures and facilities is described in the IRC document 'Security Measures: Definitions'.

exactly how the requirements will be met, but rather what performance will be delivered. This makes it possible to select the most suitable solutions among the various (and many) security options available for a certain situation.

A security plan may contain information that is partially or fully confidential. This information must not find its way into the hands of unauthorised parties. This means that only authorised persons may read this information, which persons will have signed a confidentiality agreement and will have been issued a Certificate of Good Conduct.

The implementation of the measures in a security plan in relation to working with radioactive materials is in part governed by the requirements for radiation safety. There where security measures and facilities have a negative effect on the radiation protection measures, the radiation protection measures will prevail and alternatives will thus need to be found for the security measures (‘safety first, security follows’).

If a BORG security certificate is to be requested, then the current versions of the IRC source documents must be adhered to. The security principles must be recorded in a schedule of requirements. To avoid differences of opinion, all involved parties must declare in writing that they agree with the security plan and its principles. It can be agreed that the operational inspection will be performed by a body that is certified to inspect and certify security systems if one of the involved parties so desires or requires it.

4.5 Extraordinary situations

If an extraordinary situation presents itself, parties may decide to draw up an alternative security plan. This will involve made-to-measure solutions for which three situations are conceivable:

(1) the radioactive materials are located in only part of the property or part of the property falls under a higher category;
(2) the entire property requires made-to-measure security;
(3) the radioactive materials are located in a nuclear plant.

In the first case it may be sufficient to only secure the most high-risk part of the property. This is a case of partial security of the property, so that the system as described in 4.2 and 4.3 can be used for determining the security measures in principle. If this system is followed, then a ‘standard’ BORG security certificate can be issued for the secured property (or part of the property). Some conditions do apply, which are described in the IRC document ‘Security Measures: Definitions’.

In the second case it may be that a part of the property where concentrations of radioactive materials occur (storage) falls under a higher risk category than the remaining part of the property (offices and/or production areas). In this case, a package of measures will need to be determined that takes account of the various risks in the various parts of the property.

In the third case, the Plant Security Manager of the nuclear plant will need to be contacted and asked to draw up a security plan.

The ‘standard’ security measures defined in the security categories will not always lead to an optimum result. In some situations it may be better to put together an alternative package of security measures. This can be done by following the ‘equivalence’ principle.

This entails applying measures that have a combined result that is ‘equivalent’ to the result of the measures prescribed in the relevant security category. This is relatively simple where it concerns products, structures or facilities for which standardised tests or regulations exist. These measures can then be assessed on the basis of the test results or the relevant regulations. Where this is not possible the assessment will need to be made based on expert knowledge and experience. If a BORG security certificate is to be requested where the equivalence principle has been applied, it is important that the directly involved parties have reached agreement beforehand. This is done by recording the made-to-measure solutions in the schedule of requirements which is then signed for approval by the involved parties.

5 Practical examples

The first example is used to further explain a number of relevant security principles. This will be followed by two practical examples that illustrate how relatively simple and inexpensive it can be to secure property against theft.

5.1 Permanent storage of radioactive materials

Situation:

Permanent storage of teletherapy equipment in a hospital radiology room. The security desk is a 4-minute walk from this room. The police station is an 8-minute drive from the storage location and the hospital is registered as a CBRN business.

Risk analysis:

The location is a permanent storage area for radioactive materials. Teletherapy equipment is classified in category 1 in the Ministerial Regulation on the Security of Radioactive Materials. This corresponds with IRC risk category 4. The teletherapy equipment must thus be secured according to IRC security category 4.

Security measures:

O	P	E	R	Comments
O2	P3	E3	R3	Perimeter detection level 2 Perimeter detection near storage area level 3
Or				
O2	P2 + C/U2	E3	R3	Perimeter detection level 2
Or				
O2	P1 + C/U3	E3	R3	-

These combinations of security measures and facilities can be used in accordance with IRC risk category 4. This means that there are a number of choices possible for the security of teletherapy equipment.

The choice of a particular mix of security measures is determined by the following factors:

- the effectiveness of the mix of measures (an absolute prerequisite for security is that the chosen measures and facilities actually work in in practice);
- the investment required to purchase the requisite security equipment and/or equip security personnel;
- the operational costs of the security systems (including personnel costs);

- the possibilities for expansion of the security technology/system to be applied;
- the condition that new equipment or a new system must be able to be used in conjunction with or as an extension of an existing system.

Timeline analysis:

The best combination of security measures can be determined by performing a timeline analysis (PICE/ALRE). The timelines are then used to analyse a scenario. By performing timeline analyses of various security solutions on paper, the involved parties can ascertain which solutions do and do not meet the requirements and even which is the optimum solution for a certain situation. The effectiveness of the mix of measures determines the final choice. If only one of the options described above results in a positive security yield (sufficient security), then this will be the mix of measures to adopt. If more than one combination of security measures is possible, then the next step will be to compare the investments and operational costs involved. Often, the most inexpensive mix of security measures will be the logical choice.

Mix of security measures and timeline analysis:

1. Organisational measures:

In this situation the O measures are all the same: O2. So the choice of organisational measures is simple.

O2 means:

- standard organisational measures (locking plan, lighting, schedules, etc.);
- information provision on prevention in the broadest possible sense;
- the requirement to include organisational measures in the security plan.

2. Physical measures:

The starting point for physical measures is that they take account of the principle of 'safety first, security follows'. In this situation, the categories P1, P2 and P3[10] are all available, but two of these must be combined with other measures: P1 with C/U3 and P2 with C/U2.

- P1 means: the implementation of physical measures aimed at a hold-up time of 3 minutes in accordance with BRL 3104[11] (= modifying door and window furniture) or in accordance with resistance class 2 in NEN 5096.
- P2 means: the implementation of physical measures aimed at a hold-up time of 5 minutes (resistance class 3 in NEN 5096). In an existing situation, P2 can also be achieved by installing additional mechanical measures such as grilles, roll-down shutters or security glazing.
- P3 means: the implementation of physical measures aimed at a hold-up time of 10 minutes (resistance class 4 in NEN 5096[12]) or the installation of roll-down shutters, grilles and/or security glazing.

10When physical measures are installed at level P1, P2 and P3 then lock cylinders shall be in the same category as the lock. Certified lock cylinders are compulsory for compartment doors. This is recommended for all main and secondary access doors.

11National assessment guideline for KOMO product certification for burglary-resistant door and window furniture on windows, doors and hatches.

12This standard describes the requirements, classification and testing methods for burglary-resistant doors, windows, frames, skylights and the relevant structural components.

Essentially, these physical security measures are aimed at achieving a minimum hold-up time of 3, 5 or 10 minutes respectively. A longer hold-up time can be achieved by installing proportionally stronger physical security measures, but this entails a relatively larger investment.

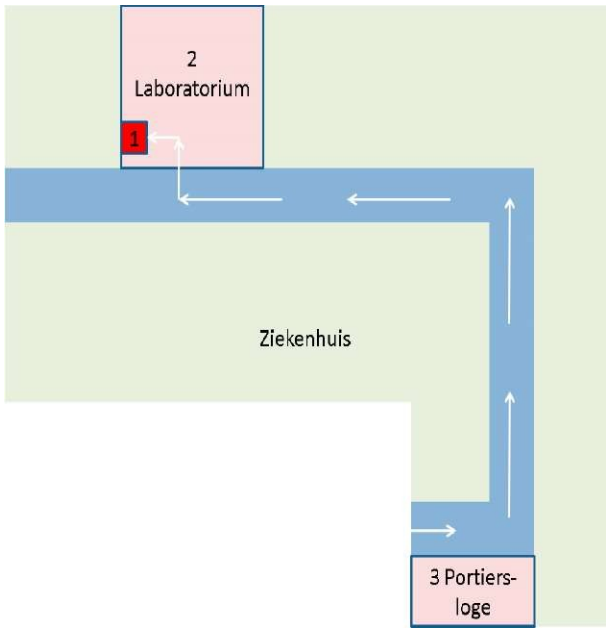
What is the outcome of a choice for P1 + C/U3 or P2 + C/U2?

- C/U2 means: the installation of compartmentalisation or unauthorised removal prevention measures such as a secure cabinet or safe in accordance with the requirements of the VGW trade association, secure showcases, fences or rolling gates. The performance requirement is a hold-up time of 5 minutes.
- C/U3 means: the installation of compartmentalisation or unauthorised removal prevention measures such as a secure cabinet or safe in accordance with the requirements of the VGW trade association, a safe or a mist generator. The performance requirement is a hold-up time of 10 minutes.

The hold-up times of the various options are as follows: P1 + C/U3 3 +10 = 13 minutes P2 + C/U2 5 + 5 = 10 minutes P3 10 minutes

The various facilities may be ‘added up’. This means that the combination of P3 + C/U2 results in a 15-minute hold-up time; a combination of 3 doors in a row that each provides a delay of 5 minutes results in a total hold-up time of 15 minutes. However, some combinations will not have a meaningful result.

If it is not possible to achieve an adequate hold-up time, for example because the physical measures required are financially infeasible, or because physical measures cannot be installed due to safety considerations, then barriers (such as fencing) around the periphery of the storage area can be considered for increasing the hold-up time.



3. *Electronic measures and response (alarm response):* The requirements placed on electronic (E) measures and the response (R) are described in detail in the IRC document ‘Security Measures: Definitions’. For the sake of brevity we refer to this here.

Choosing the right mix of measures:

All the information required to choose a mix of measures has been gathered. We can now design a security plan on the basis of this information. In order to calculate the required hold-up time, we first make a list of the known data on the alarms, alarm verification and response (ALRE).

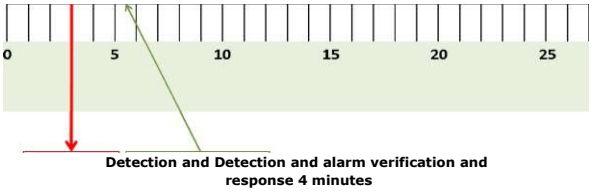
The required hold-up time depends on the security category in accordance with the Ministerial Regulation on the Security of Radioactive Materials.

After an alarm has been generated - and thus the security desk has been alerted - the time required for alarm verification and the first response by the security guard is 4 minutes at the most. This means that the hold-up time must be more than 4 minutes for a positive security yield.

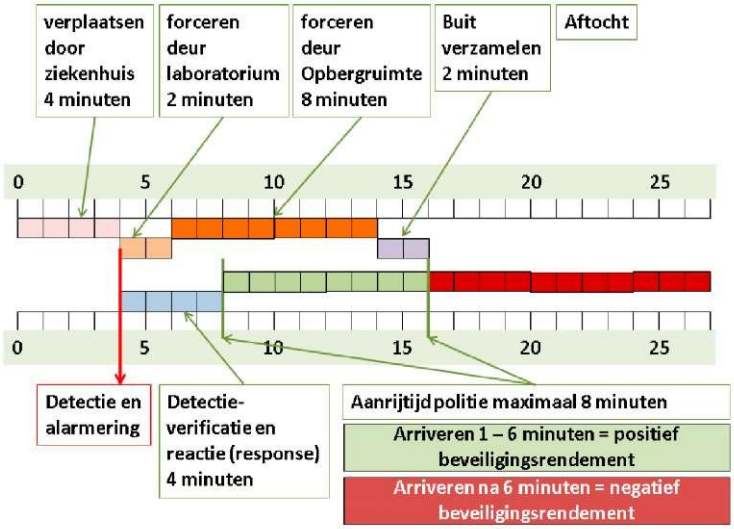
Generally speaking, this hold-up time will be determined by, for example:

- the distance that the offender must travel to get to his target after he has been detected. The hold-up time is influenced by aspects such as the accessibility of the terrain, the tools required by the offender to break in and steal the target, the time of day (daylight, twilight, night) and the weather. The scenarios described using the timelines must take account of these aspects;
- the barriers placed on the offender’s route. A tall, thick and thorny hedge will slow an offender down considerably;
- the construction of the storage area. A wooden structure is easier to gain access to than one made of bricks or reinforced concrete. The door furniture used (hinges, locks, etc.) must have the same strength class as the structure itself (weakest link);

- detection of the offender. If the offender is not detected - and so no alarm is generated - the offender will have as much time as he needs to perform the burglary. Likewise, if there is no alarm response then the offender will have all the time he needs.



If we choose the option O2, P3, E3 and R3, this results in the scenario below. This is a case of sufficient security (positive security yield). Two comments can be made here.



1) The appearance on the scene of a security guard can of itself be sufficient to force the offender to flee.

2) The timely arrival of the police cannot be guaranteed. The police's incident prioritisation system may lead to this intruder alarm being given less priority than other alarms received at the same time. The result will be that the police will arrive at the scene too late to arrest the offender.

This example[13] assumes that the doors and windows have the same structural strength as the brickwork walls. The other two mixes of security measures result in similar timeline scenarios.

5.2 Encapsulated sources in Non-Destructive Testing (NDT)

This example concerns the use of encapsulated radioactive sources for conducting tests of, among others, structural soundness (gammagraphy).

The tests can be conducted in specially created areas on the NDT company's premises, but also at a client's own locations. In this example, radioactive sources are transported to a client's location by a vehicle. For reasons of safety, there is always a company supervisor on hand during activities with radioactive sources. This is prescribed in the NDT company's Nuclear Energy Act license.

13
This example contains an incorrect calculation of the security yield. This is positive if the police arrive within 1-8 minutes and negative if the police arrive after 8 minutes.

When they are not being used, the radioactive sources are stored in a room that is accessible through only a single door. The storage room in this example is in a warehouse which can be accessed through a number of doors.
The warehouse stands with many others on a fenced-off site. Offenders who wish to steal the sources will need to break through at least three barriers in order to get to them, being the site fence and the doors in the warehouse and to the storage room.

If the offenders wish to gain access to the sources by using force then it will take them several minutes, depending on the strength of the barriers and the tools that they use. In order to respond to a break-in in time, it will need to be detected first. If the offenders are detected at the first barrier and this is responded to immediately, then they may be prevented from taking the next barrier. However, if the offenders are only detected after the third barrier, then they will be able to make their getaway with the stolen sources, unless additional measures have been taken to prevent this.

In this example, the sources displayed can easily be chained together with a heavy chain that is passed through the handles and then locked using a code lock. The use of a code lock means that authorised personnel are still guaranteed access to the sources (they do not need a key). These additional measures need not require major investments or high operational costs.

A variant to this solution would involve anchoring the chain to the wall for even more security. A relatively large amount of time is required for the unauthorised removal of sources secured in this manner. Timely detection followed by an immediate alarm and an adequate response to this alarm can prevent the theft of these sources.

5.3 Brachytherapy in a hospital

This example concerns the security of a brachytherapy device that is used to treat cancer. Patients are treated in a separate room that is fitted with a sliding door that meets all the applicable safety requirements. From a security perspective, this door ensures a considerable hold-up time due to its solid construction.

The room is in a nursing ward where staff (such as physicians, nurses, technicians, health physicists and cleaners) may be found 24/7. When no patient is being treated, the room can be considered as the device's storage area.

While a therapy is underway, the room is accessed by operating the door electronically. The door can only be opened if the door control is first released using a key, which is stored elsewhere. While the device is in use (i.e. when a patient is being treated), there are always medical staff present to supervise.

When the device is not being used, the room also functions as the device's storage area. In this case too, the room is closed and only accessible by operating the door electronically. The door can only be opened if the door control is first released using a key, which is stored elsewhere. There is no direct supervision when the device is not being used. Nor is there any security in place to monitor the people accessing the ward (it is a public space).

This means that, when in storage, a detection system is required to detect offenders who could force the door to access the device.

Additional security measures are also required to increase the hold-up time such that there is a positive security yield (sufficient security). For example, the device could be anchored, or it could be immobilised when not in use (if it is a portable device).

References

BS Decree of 16 July 2001, the Radiation Protection Decree. http://wetten.overheid.nl/BWBR0012702 EU01 Council Directive 96/29/EURATOM of 13 May 1996 laying down basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionising radiation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0029:NL:HTML EU02 Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union - an EU CBRN Action Plan; 15505/1/09 REV 1. http://register.consilium.europa.eu/pdf/en/09/st15/st15505-re01.en09.pdf IAEA01 General Safety Requirements Part 3 (Interim). Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards. http://www-pub.iaea.org/MTCD/publications/PDF/p1531interim web.pdf IAEA02 Code of Conduct on the Safety and Security of Radioactive Sources; IAEA/C0DE0C/2004. http://www-pub.iaea.org/MTCD/publications/PDF/Code-2004 web.pdf IAEA03 IAEA-TECDOC-1344,Categorization of radioactive sources, Revision of IAEA-TECDOC- 1191. http://hps.org/documents/IAEATecDoc1344.pdf IAEA04 IAEA Nuclear Security Series No. 11, Security of Radioactive Sources. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1387 web.pdf IAEA05 E P R - D -VALUES 2006, Dangerous quantities of radioactive material (D-values). http://www-pub.iaea.org/MTCD/publications/PDF/EPR D web.pdf MR01 Regulation of the Minister of Economic Affairs of 3 December 2012, no. WJZ / 12311250, concerning rules on the security of radioactive materials (Regulation on the Security of Radioactive Materials). http://wetten.overheid.nl/BWBR0032390 VRKI01 Improved Risk Classification: Security Measures: Definitions; document D03- 385; January 2012. http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/risicoklassenindeling/vrki d ef beveiligingsmaatregelen 2012.pdf VRKI02 Improved Risk Classification for Organisations; Document D03-376; Version: 1.1; 5 January 2012. http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/risicoklassenindeling/vrki b edrijven 2012 versie1-1.pdf VRKI03 Improved Risk Classification (VRKI 2012) for homes and organisations; IRC chart http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/risicoklassenindeling/vrki-kaart 2012.pdf