IN TRANSIT STORAGE OF RADIOACTIVE MATERIAL UNDER NATIONAL CUSTOMS ADMINISTRATION

S. Fernández Moreno, C. E. Rodríguez, R. H. Cesario (1), C. Milsztain, L. Pollach, and R. Llosa (2)

(1) Nuclear Regulatory Authority, Av. Del Libertador 8250, (1429) Bs. As., Argentina
(2) National Customs Administration, Azopardo 350, (1107) Buenos Aires, Argentina

SUMMARY

A model of an "in transit storage of radioactive materials" under National Customs Administration control[1] is described account the relevant Custom House Legislation and the Nuclear Regulatory Standards[2] in force in Argentina.

Evaluation of the physical protection systems applied to the above mentioned storage by means of a software named "IntruBuster"[3] is also described. This software is routinely updated and is also used by the Nuclear Regulatory Authority to evaluate the adequacy of physical protection systems implemented at nuclear installations in the Country.

The interaction with National and International related Organisations to minimise the probability of illicit trafficking of nuclear materials is another important aspect to be considered. This is particularly true in those cases in which the administration of these stores is privately operated.

Finally, the paper describes the experience obtained in the implementation of the above mentioned software as well as prosecution and control activities by the Custom House and the Nuclear Regulatory Authority of Argentina.

INTRODUCTION

In order to get a good understanding of the in transit warehouse model under the Custom House control, the primary and secondary zones of such stores are briefly described.

Primary Zone: Is part of the customs house territory area, e. g., terrestrial, aquatic and aerial space in which same tariff system and economic prohibitions to import and export materials are applied (customs operations carried out in this zone are under custom house control). In this zone, special rules for people and merchandise movement and disposal, are applied. This zone includes:

- sites, installations, stores and places where customs house operations or controls take place;
- ports, wharves, airports and border accesses;
- aquatic areas as bays and ports which are adjacent to the above mentioned places;
- the rest of the areas bounded to similar functions than the previous ones; and
- the corresponding air spaces.

Secondary Zone: Is the customs house territory excluded from the primary zone. The Article 280 of the Customs Code of Argentina[1], states that the merchandise whose storage implies a danger for the safety of people must be secured.

TYPICAL FEDERAL WAREHOUSE

Is a covered or uncovered area to be accessed from any internal or external point from the warehouse or from any sector, without trespassing the custom secondary zone.

FEATURES

- Area Size: in accordance with the operation, from 1,000 to 2,000 m^2.
- Limits: resistant structure wall of 2.5 m to 4 m.
- Accesses: must meet the following conditions:
  - a given size and location to allow the in and out of vehicles as well as his indoor loading/unloading procedures from and to the federal warehouse;
  - at least, one of the accesses to the federal warehouse, must allows the direct entry from the outside, in order not to cross the custom secondary zone. We have to distinguish between operative and non-operative accesses:
    - the use of the operative access is for the entry and exit of merchandise to and from the federal warehouse in normal operative conditions, and the use of the non-operative access is to blockade;
    - only one access to the federal warehouse will be allowed. In case that more operative accesses are required, it must have an exit control.

- Floor Structure: illumination system must be appropriate to allow a correct federal warehouse operations.
- Verification Sector: The federal warehouse must have a proper delimited sector to perform the verifications, inspections, and other similar operations.
- Repackaging Sector: The federal warehouse must have a proper delimited sector to perform repackaging operations.
- Consolidations Sector: If the federal warehouse carries out export operations a proper delimited sector to perform the consolidations will be required.

"The mentioned three sectors (to perform the verifications, repackaging and consolidations) must be perfectly separated and delimiting from each other".

- The offices for custom service are as follows:
  - located in such way to see the federal warehouse operative access, in order to let the custom staff control the persons and goods access;
  - have an effective communication channel with the operative sector of the federal warehouse, e.g.: the verification sector;
  - have the appropriate computing equipment to have access to the "María Computing System " used by Argentinean Customs House; and
  - have, as a must, a CCTV to control the several sectors of the federal warehouse.

EVALUATION OF PHYSICAL PROTECTION SYSTEMS

The System of Physical Protection of Nuclear Material and Installations in Argentina started at the very beginning of the nuclear activities and has been improved since then. Nowadays, the Department of Physical Protection, within the Nuclear Regulatory Authority (ARN) of Argentina, is responsible to carry into effect the ARN Basic Standard[2]. This standard is applied to thirty three (33) installations in the whole country.

The ARN uses a computerised model named "IntruBuster"[3] to evaluate the physical protection system of federal warehouses. This evaluation is performed through a graphic model of the installation where the information about distribution of different sectors, detection elements, delay elements, modality of intruder access and security force response time are included.

BASIC CONCEPTS

The most important concepts of the implementation of the security analysis of nuclear installations are now described. The security evaluation of a physical installation requires a computational tool to estimate the vulnerability against an intruder who wants to achieve a given target. The distribution of physical elements to prevent the intruder access has to be modelled in an appropriate way.

ANALYSIS METHODS

It is important to mention that the first model for security assessment was the "IntruBuster"[3]. The new version uses two types of analysis: an Analysis by Levels and a Monte Carlo Analysis.

ANALYSIS BY LEVELS

The first version of "IntruBuster"[3] worked with the **"Analysis by Levels" method**. It makes an abstraction of the installations where the areas and accesses are basically the same element. These elements connect the different levels (reduced to points without dimension) of the installation in a linear structure obtaining a simple and fast analysis. However, the analysis is not so realistic when the installation has a high degree of complexity. This method is not suitable in cases where the complexity of the installation doesn't make possible the applicability of a scheme of nodes and accesses.

ANALYSIS BY MONTE CARLO METHOD

With the "IntruBuster"[3] programme it is possible to build the model directly from the installation layouts. The elements, which are involved in the security of installation (delay and detection elements), are joined in regions (areas, accesses, levels, etc.) that are represented on the design window.

The **Monte Carlo method** allows us to take into account the spatial and temporal information from the installation, and the user only has to input the real information. The method consists in the simulation of "intruders" whose appearance, circulation and movements "inside" the diagram are completely at random. In this manner, a number of "intrusions" are automatically generated. Some of them will result in the capture of the intruders, others in the neutralisation and some in the successfully reaching of the target. From all these possible paths, some of them will be the most vulnerable. Finally, there are some parameters of forward, backward and lateral movement that characterise the behaviour of the intruder in their action of reaching the target.

One important tool is the use of a **Vectorial Method.** Through the movements of the cursor, it is possible to change the position of access, detection and delay elements, guard room and target room on the installation layout and to obtain other performance of the physical protection system. The main purpose for this is to get the best configuration of the physical protection system of the installation with the maximum interruption probability.

The previous mentioned "analysis by level" method shows only the interruption probability while the Monte Carlo method is more effective due to the use of the "random" feature. This feature lets the analysis arrive at a more accurate result yielding a final report showing the interruption probability and the critical time.

PENETRATION PATHS TO THE TARGET

The possible penetration path is any path the intruder can access through in order to reach his target. Provided the Security Force Response Time (SFRT) is faster than the intruder's access time, the target may or may not be reached.

CRITICAL DETECTION POINT

The Critical Detection Point is the intruder's point in a given path where he must be detected to prevent the reaching of his target. But as mentioned before, this point also can be met provided that the response time is faster than the intruder's time to the target.

Whether this point can or can not exist, it depends on the SFRT be faster or slower than the intruder access time to the target.

NON-DETECTED INTRUSION PROBABILITY

Two types of elements compose the diagram: detection and delay. The calculation of probabilities basically takes into account the Non-Detected Probability (the probability

of an intruder to access the area where the detection is taking place and not be detected). Associated with each element of detection, and also with the temporal information of the delay elements, there is an evaluation of the Interruption Probability. Each i-access or i-area has j elements of detection, which can be found in one of the k possible paths to the target. The probability that the intruder won't be detected in a given access or area is equal to the probability that no detection elements can detect him. Then:

P(i-area or i-access non-detected) = P(no det 1 and no det 2 and ... and no det n)

TOTAL AND CRITICAL NON-DETECTED PROBABILITY

There are two quantities to be evaluate in all the possible paths. The first, is the probability of the intruder to reach the target without been detected along the path. The second, is the non-detected access probability until the CDP is reached.

INTERRUPTION PROBABILITY

From all the possible paths, the most vulnerable is the one where the critical probability is maximum. The IP will be the complement of the maximum Critical Probability, in other words, the probability that an intruder be detected before or in the CDP for the most vulnerable path:

$$IP = 1 - CP_{MAX}$$

DELAY

The Delay is the temporal time the intruder takes from the access path to the target. This temporal time can be set up through any device specially designed to detect any material elements that come across the path (obstacles, walls, etc..), or simple by the elapsed time along the way.

Another possibilities are the actions the guards may take. To evaluate the Non-Detected Penetration Probability we have to compare the Total Delay -from the Critical Detection Point to the target- against the Security Force Response Time and thereby get the Interruption Probability.

CRITICAL PATH

The Critical Path is the one with the most Non-Detected Penetration Probability or, in other words, the path with the lowest IP.

DETECTION

The detection is an action caused by the intruder in an area of the installation where special devices are located to detect the intruder's presence. The detection elements can be completed with additional conditions to validate or not the chosen option (e.g., presence or absence of security guards).

SECURITY FORCE RESPONSE TIME

This is the time that the Response Force takes to intercept the intruder after his detection. The Security Force Response Time often is not a unique value to take into account, it depends on the location of the Security Force with respect to the different areas where the intruder can be captured. Each area of the installation has to have a Security Force Response Time. The "IntruBuster[3] software uses two types of values for the SFRT:

- the "Global" one, which is the input to the software "Buildings" window and represents the time the Security Force takes to get from the exterior to the installation;
- the "Local" one, which is the input to the software and represents the elapsed time the security force takes to get from the exterior through different areas to a specific point.

Therefore, the "Effective" SFFRT from each area is the sum of the global and the local values:

$$\text{Effective SFRT} = \text{Global SFRT} + \text{Local SFRT}$$

NUMBER OF INTENTS

The number of intents is the number of iterations that the Monte Carlo analysis runs on the installation. We need a given number of iterations to converge to the critical path, and this given number depends on the complexity of the installation and the value of the forward, backward and lateral displacements of the intruder. An approach to the method is described as followed:

- to use a number of iterations less or equal than 40 x number of areas;
- to run the analysis three times with the recommended number of iterations and check for convergence.

If convergence isn't obtained, we have to increase the number of iterations and/or modify the probabilities of forward, backward, and lateral displacements.

MENUS

There are a lot of menus one can use in this software. These menus are related to:

- Managing the files
- Set the buildings, images and devices
- Running the analysis
- Showing the results of the analysis
- Showing the pictures from the installations

TECHNICAL DETAILS

The "IntruBuster"[3] programme has been developed in the Microsoft Visual Basic®

language. This programme is aimed at processing data and screen images at different stages, and the Microsoft® Access Database is aimed at storage the required data. For a better software performance, the following hardware is required:

- PC Pentium 133 MHz
- 16 Mbytes RAM
- Windows® 95 Operating System

CONCLUSION

The international co-operation on this subject is particularly necessary in those situations involving the movement of nuclear and/or radioactive material across the borders. In this context, the adequacy of the physical protection measures and the control customs adopted by the Argentine State have special relevance. In our particular case, we consider that such measures contribute to minimise the probability of such events.

REFERENCES

(1) Argentine Law 22.415, Art. 280 Argentine Customs Code
(2) Basic Standard AR 10.13.1 "Physical Protection of Materials and Nuclear Installations"
(3) "IntruBuster" programme (Version 1.0 and 2.0)