Hungarian Atomic Energy Authority

(This is an unofficial translation of the text)

Guideline PP-9

Evaluation of the effectiveness of the physical protection system of nuclear facilities (with the exemption of those operating reactor having less than 1 MW thermal power), and radioactive waste temporary storage and final disposal facilities

Version number:

2.

September 2015

Issued by:

Gyula Fichtinger

Director General of the HAEA

Budapest, 2015

The publication can be acquired from:

Hungarian Atomic Energy Authority

Budapest

FOREWORD FROM THE DIRECTOR GENERAL

The Hungarian Atomic Energy Authority (hereinafter referred to as HAEA) is a central state administration organ (a so-called government office) having nation-wide competence in the field of peaceful use of atomic energy; it operates under the direction of the Government, it has independent tasks and scope of authority. The HAEA was established in 1990 by the Government of the Republic of Hungary with Govt. decree 104/1990. (XII. 15.) Korm. on the scope of tasks and competence of the Hungarian Atomic Energy Commission and the HAEA.

The public service of the HAEA as defined in law is to perform and coordinate, independently of organizations having interest in the application of atomic energy, the regulatory tasks in relation to the peaceful and safe use of atomic energy, including the safety of nuclear facilities and materials, nuclear emergency response and nuclear security, and the corresponding public information activity, and to make proposal to develop and amend, and to offer an opinion on proposed legislations corresponding to the use of atomic energy.

The fundamental nuclear safety objective is to ensure the protection of individuals and groups of the population and of the environment against the hazards of ionising radiation. This is ensured with effective safety measures implemented and adequately maintained in the nuclear facility.

The radiation protection objective is to keep the radiation exposure of the operating personnel and the public all times below the prescribed limits and as low as reasonable achievable. This shall be ensured in the case of radiation exposures occurring during design basis accidents, and as far as reasonably possible during beyond design basis accidents and severe accidents.

The technical safety objective is to prevent or avoid the occurrence of accidents with high confidence, and the potential consequences occurring in the case of every postulated initiating event taken into account in the design of the nuclear facility shall remain within acceptable extent, and the probability of severe accidents shall be adequately low.

The HAEA determines the way how the regulations should be implemented in guidelines containing clear, unambiguous recommendations in agreement with the users of atomic energy. These guidelines are published and accessible to every members of the public. The guidelines regarding the implementation of nuclear safety, security and non-proliferation requirements for the use of atomic energy are published by the director general of the HAEA.

Hungarian Atomic Energy Authority

FOREWORD

The internationally accepted bases of physical protection are represented by the Law Order 8 of 1987 on the promulgation of the International Convention on the Physical Protection of Nuclear Materials, the Act LXII of 2008 on the promulgation of the Amendment to the Convention on Physical Protection of Nuclear Materials approved in the frame of the International Atomic Energy Agency and promulgated by Law-decree 8 of 1987 amended by a Diplomatic Conference organized by the IAEA signed on July 8, 2005, and the Act XX of 2007 on the promulgation of the International Convention for the Suppression of Acts of Nuclear Terrorism.

The realization of the stipulations undertaken by Hungary, at the highest level, is represented by the Act CXVI of 1996 (hereinafter referred to as Atomic Act), which includes the fundamental security principles and establishes the frame of the detailed physical protection regulations.

The Govt. decree 190/2011. (IX. 19.) Korm. published based on the authorization of the Act (hereinafter referred to as Government Decree) establishes the legal requirements for the physical protection of the use of atomic energy and for the connecting licensing, reporting and inspection system.

The HAEA is authorized to develop recommendations regarding the implementation of requirements established in laws, which are published in the form of guidelines and made accessible on the website of the HAEA.

For the fast and smooth conduct of licensing and inspection procedures connecting to the regulatory oversight activity, the Authority encourages the licensees to take into account the recommendations of the guidelines to the extent possible.

If methods different from those laid down in the regulatory guidelines are applied, then the Authority shall conduct an in-depth examination to determine if the applied method is correct, adequate and full scope, which may entail a longer regulatory procedure, involvement of external experts and extra costs.

The guidelines are revised regularly as specified by the HAEA or out of turn if initiated by a licensee.

The regulations listed are supplemented by the internal regulations of the licensees and other organizations contributing to the use of atomic energy (designers, manufacturers etc.), which shall be developed and maintained according to their quality management systems.

Before applying a given guideline, always make sure whether the newest, effective version is considered. The valid guidelines can be downloaded from the HAEA's website: http://www.oah.hu.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Scope and objective of the guideline

The guideline contains recommendations on how to comply with the regulations established in the Government decree.

This Guideline aims at clarifying the regulatory requirements established in Section 30 of the Government decree for the establishment of the physical protection system of nuclear facilities (with the exemption of those operating reactor having less than 1 MW thermal power), and the radioactive waste temporary storage and final disposal facilities.

The Government decree requires that:

"Section 30

The obligant shall realize the physical protection of the nuclear facility, except for that equipped with a nuclear reactor of less than 1 MW thermal power, interim storage and final repository of radioactive waste, such a way that ensure the effective protection against the design basis threat prescribed for the specific facility by regulatory decision."

In addition to providing adequate protection against the Design Basis Threat (hereinafter referred to as DBT), the physical protection system shall comply with the minimum requirements as defined in Section 5-7 of the Govt. decree for the use, storage and transport of nuclear materials, radioactive sources and processing, storage and transport of radioactive wastes.

In the case of nuclear facilities (with the exemption of those operating a reactor having less than 1 MW thermal power), and radioactive waste interim storage and final disposal facilities the target of a sabotage can be not only the nuclear materials, radioactive sources and radioactive wastes, but those systems and components, which have importance from the viewpoint of radiological consequences. Accordingly, Section 7 (6) of the Government decree regulates that:

"*(6) Concerning systems, structures and components significant to radiological consequences the level of physical protection shall be identical to that of the used or stored nuclear material and radioactive source, or processed, disposed radioactive waste, determined according to Sections (1)–(5).*"

The compliance with the above requirements is verified by the Authority through the authorization of the physical protection plan and the inspection of the functioning of the system established. The functional performance is assessed in reflect to the facility specific Design Basis Threat as defined by the State for nuclear facilities (with the exemption of those operating a reactor having less than 1 MW thermal power), and radioactive waste interim storage and final disposal facilities.

This Guideline establishes the principles of the evaluation of the effectiveness of the physical protection system in reflect to the Design Basis Threat, and thus supports the design of the physical protection system as well as the compliance with the criteria for the operation of the system.

1.2. Corresponding laws and regulations

The legal background of the nuclear safety requirements is established in the Atomic Act and the Government decree.

2. TERMINOLOGY

This guideline used the following terminology in addition to the terms determined in Section 2 of the Atomic Act and Section 2 of the Government decree.

Response time (TRF):

The period required by the response force having sufficient number and capabilities to reach the location of the adversaries and to take the position needed to deny their action, subsequent to the assessed detection and successful alarming.

Adversary pathway:

A sequence of paths of actions committed by external adversaries or insiders (as defined in the Design Basis Threat), which is needed for accessing the target of unauthorized removal or sabotage.

Unacceptable radiological consequence:

The consequence of a sabotage against a nuclear facility, nuclear material, radioactive source or radiative waste is unacceptable, if it causes or may cause a nuclear emergency; and if the sabotage entails significant exceedance of the dose limit of certain individuals or a group of individuals, or it can induce such overexposure.

Probability of intervention (PI):

The cumulative detection probability of the critical pathway, if a response force having sufficient number and capabilities is available.

Authority:

The HAEA and the Hungarian Police Headquarters.

Assessed detection probability (PAD):

The probability of detection of an overt or covert action of the adversary, which includes the operation and sensing of the given sensor, the transmittal and indication of the signal on the place of assessment, the assessment of the alarm signal, confirmation of its reality and successful alarming of the response forces.

Critical detection point (CDP):

A specific detection point of the adversary pathway, subsequent to which the cumulative delay time just exceeds the time needed for intervention.

Critical pathway:

The adversary pathway, where PD is the lowest.

Cumulative detection probability (P_D):

The probability of detection of the adversary, prior to passing the critical detection point.

Cumulative delay time (T):

The sum of the delay times (Ti) of the components of the physical protection system subsequent to a given detection point on an adversary pathway.

Minimum cumulative delay time (T_{min}):

Cumulative delay time on the adversary pathway subsequent to CDP.

Probability of neutralization (P_N):

The probability of neutralization by the response forces after timely arrival before the adversaries reach their target.

3. RECOMMENDATIONS OF THE GUIDELINE

3.1. General considerations

(1) In the case of sabotage against nuclear facilities, the evaluation of the effectiveness of the physical protection system should be based on the functional performance in reflect to the Design Basis Threat.

(2) The physical protection system should prevent the access to the sabotage target on any pathway by adversaries having the number and capabilities as defined in the Design Basis Threat. A basic condition for reaching this goal is the proper functioning of the response function of the physical protection system. The effective functioning of the response function is determined by its two elements: the timely denial/intervention and the successful elimination.

(3) The timely denial/intervention is dependent on the performance of the deterrence, detection, delay and response functions of the physical protection system. From the viewpoint of timely denial, the physical protection system should be characterized by the probability of denial/intervention (P_I). However the probability of denial/intervention is determined by the effectiveness of the components belonging to the detection function and the time need of the response (as discussed below). Additionally, the deterrence function of the system has relevant role as well, thus the establishment of the highest level of deterrence is justified for protection against sabotage.

(4) The success of elimination of a given adversary force is dependent on the size and tactics of the response forces. The response forces should be able to eliminate the adversaries. Accordingly, the physical protection system is usually characterized by the probability of neutralization (P_N). This Guideline proposes the determination of the conditions for elimination based on a deterministic approach; therefore it is assumed that the elimination is successful after denial ($P_N = 1$).

(5) The physical protection system should ensure that the product of denial/intervention probability against an attack defined in the DBT on the critical pathway (P_I) and the neutralization probability (P_N) should not be smaller than the value defined in this Guideline with regard to a given type of facility.

3.2. Assessment of the effectiveness of the physical protection

system

3.2.1. Determination of the response time (T_{RF})

An important character of the physical protection system is the time period required by the response force(s), subsequent to receipt of an alarm after detection, to reach a specific point and take the positions needed for denial.

The response time is the sum of the average time periods needed for the achievement of the below actions:

1. Transmission and indication of the alarm signal induced by detection to the location of assessment.
2. Assessment of the alarm signal.
3. Alarming of the response force(s) (guards, special forces, police, etc.) in sufficient number with sufficient capabilities.
4. Preparation of the response force(s) for action.
5. Arrival of response force(s) to the point of action.
6. Taking of the positions needed for successful denial.

3.2.2. Identification of the Critical Detection Point (CDP) of the adversary pathway

Those detection points should be identified along a given adversary pathway, where the subsequent cumulative delay time (T) is greater than the response time of the response force (T_{RF}). The detection point associated with the smallest cumulative delay time (T_{min}) will be the critical detection point; consequently, the system should detect the adversary until this point in order to perform successful denial. Accordingly, the value of T_{min} should be greater than T_{RF}.

3.2.3. Determination of the shortest cumulative delay time (T_{min}):

The delay times characterizing the elements of the pathway can only be determined with certain uncertainties; therefore the above mentioned comparison can be judged at a certain reliability level on probabilistic basis.

Following the principle of conservatism, the following deterministic approach is proposed instead of the probabilistic analysis. An uncertainty interval of 30% (as internationally suggested for human actions) was assumed for the anticipated values of certain time periods (i.e. $\overline{T}_i$, $\overline{T}_{RF}$); thus T_{min} and T_{RF} should be calculated as follows:

$$T_{\min} = 0{,}7 \cdot \sum_i T_i \qquad \text{[E.1a]}$$

$$T_{RF} = 1{,}3 \cdot \overline{T}_{RF} \qquad \text{[E.1b]}$$

The delay is sufficient if $T_{min} > T_{RF}$.

The average delay times for components performing the delay function, which are dependent on the tool used by the adversary, are compiled in Guideline PP-4.

3.2.4. Determination of the cumulative detection probability (P_D):

The cumulative detection probability (P_D) along a given adversary pathway should be calculated from the assessed detection probability (P_{AD}) of the sensors located in front of the critical detection point, as follows:

$$P_D = 1 - \prod_i \left(1 - P_{ADi}\right) \qquad \text{[E.2]}$$

The characteristic values of assessed detection probabilities (P_{AD}) for the most widely used sensor types, dependent on the actual conditions of application, are compiled in Guideline PP-3.

Consequently, the cumulative detection probability (P_D) is the probability that the system detects the adversary before the cumulative delay provides sufficient time for the response. This point is called as the Critical Detection Point (CDP). This characterization of the physical protection system is called as the concept of timely detection.

From this aspect, any delay performance before the first positively assessed detection has no real impact, since the alarm of the response forces starts only after the first detection. The pathway, where the (P_D) is the smallest, is the critical pathway.

The above described approach is presented in the Figure below, where the adversary should perform 8 successful actions (i.e. to jump over the fence, run to the next fence, penetrate through fence, run to the buildings, penetrate to the buildings, etc):

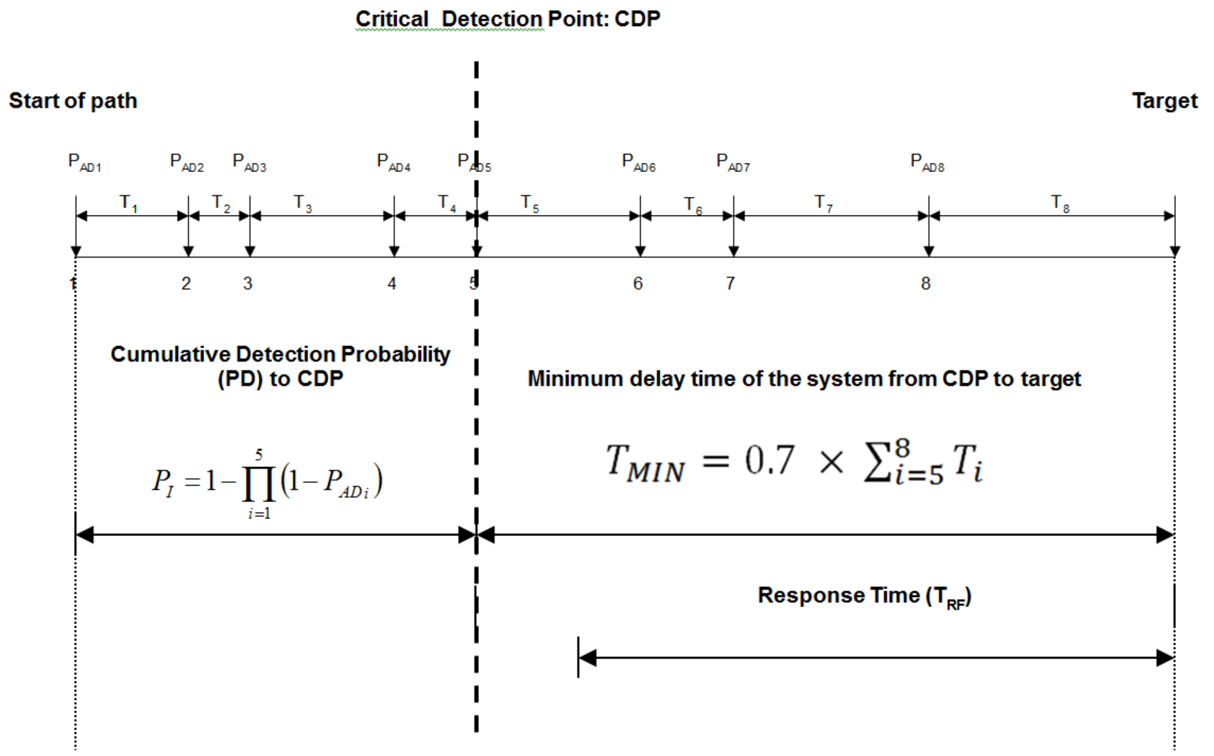

Figure 1. Schematic diagram of an 8-step adversary pathway

Figure 1 reveals that the detection point belonging to Step 5 is the Critical Detection Point (CDP) along this specific pathway, since subsequent to this point the cumulative delay time of the system still exceeds the response time of the response forces.

3.2.5. Determination of denial/intervention probability (P_I)

The entire physical protection system should be characterized by the smallest value among the individual $P_{D,j,k}$ values determined according to the above approach to all the potential targets (j) and adversary pathways (k):

$$P_I = \min\left(\sum_j \sum_k P_{D,j,k}\right) \quad \text{[E.3]}$$

Accordingly, the steps how to determine the denial/intervention probability characterizing the physical protection system (P_I) are as follows:

1. Identification of targets that are critical from sabotage point of view (total number: j), based on the categorization of nuclear and other radioactive materials as described in Guideline PP-1. Potential critical targets are the

nuclear materials in Category I and II, the radioactive sources in Category 1, the radioactive wastes in Category 1 and the systems and components significant to radiological consequences.

2. Determination of all the possible adversary pathways to each target (total number: j x k).
3. Determination of the Critical Detection Points (CDP) and the cumulative detection probabilities ($P_{D,jk}$) on each individual adversary pathway (j,k).
4. Determination of the minimal $P_{D,jk}$ and the critical pathway.

3.2.6. Probability of neutralization of the physical protection system (P_N)

An important feature of the physical protection system is the probability of neutralization (P_N), which provides the probability that the response forces are capable to stop and neutralize the adversary forces defined in the DBT after the intervention before they reach their target.

Statistically, P_N can be defined as the ratio of the number of winning attacks (G) and the total number of attacks (N) made under identical initial conditions (i.e. number of attacking forces, their location, weapons and tactics, etc):

$$P_N = \frac{G}{N} \qquad [E.4]$$

The probability of neutralization should be determined by the use of the approaches listed below:

a) expert judgement
b) simple numerical calculation
c) computer modelling (strategy games)
d) results of simulations and exercises.

Based on international experience, the neutralization is always successful ($P_N = 1$), if the response forces available at the scene comply with each of the following conditions:

a) The number of the response force staff is at least equal to the number of adversaries.
b) The weapons of the response force staff are at least as effective as the weapons of the adversaries.
c) The response forces have taken their positions before the neutralization; what is guaranteed by the $T_{min} > T_{RF}$ condition.

3.2.7. Conditional risk of the effectiveness of the physical protection system

The conditional risk of the effective response of the physical protection system to a given intrusion (R_F) should be formulated as follows:

$$R_F = (1-P_I*P_N)*C \quad [E.5]$$

where C is the severity of the consequences of a successful adversary action. The risk is conditional, because it should be assumed during the design and analysis of the physical protection system that an adversary action will occur, thus the occurrence probability of the adversary action is assumed to be 1.0.

In practice, the optimization of the physical protection system should mean the reasonable maximization of the value of the P_I*P_N product, which is thus the measure of effectiveness.

In addition, the E.4 formula expresses the risk informed design of the physical protection system. An object having great conditional risk (great C value) should be protected with a physical protection system providing high level of protection (great P_I*P_N product).

3.3. Evaluation of the physical protection system

The effectiveness of the physical protection system against sabotage is acceptable, if the value of the P_I*P_N product reaches the below defined values for each target.

Target	P_I*P_N product
Nuclear material categories for sabotage	
I.	0.99
II.	0.95
Other radioactive material categories	
1.	0.95
Systems and components significant to radiological consequences	A value associated with the used and stored nuclear and other radioactive material, and with the processed and stored radioactive waste

3.4. Documentation of the evaluation

The evaluation should be documented in such a way that clearly shows all the input data of the calculation, and all the relevant systems and components, adversary pathways, detection probabilities and delay times characterizing the pathways, the response times belonging to the critical detection point, as well as the number and capabilities of the response force.

The documentation should include the calculation in such detail, which allows the repetition of the calculation and demonstrates that the identification of the critical pathway and the calculation of the characteristic denial probability (P_I) were correct.

All the modifications and identified deviations in the design specification or in other documents used during the construction of the physical protection system should be clearly recorded in the documentation, with reference to the cause and the source.