(This is an unofficial translation of the text)

Guideline PP-3

Detailed requirement levels for the systems, structures and components of the detection physical protection function

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 OAH.

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.

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. INTRODCUTION

1.1. Scope and objective of the guideline

This guideline contains recommendations on how to meet the provisions of the Decree.

The task of systems, structures and components of the detection physical protection function is to detect any person, object or activity that threatens the facility in a way that provide the response or, at least, deterrence to be performed as soon as possible.

The solutions and systems established for detection should correlate with the other physical protection systems applied at the given location.

This guideline provides detailed guidance and practical examples regarding the detection function of the physical protection system; thus it supports the licensees to comply with the prescribed criteria.

1.2. Relevant legislation and other documents

Legal background of nuclear security requirements are provided by the Atomic Act and the Decree and the following provisions:

1. a) Handbook on the physical protection of nuclear materials and facilities, IAEA-TECDOC-1276, 2002

2. DEFINITIONS

In addition to the definitions in Section 2 of the Atomic Act and Section 2 of the Decree, this guideline uses the following definitions:

Intrusion detection system: is such an electronic device, which is able to automatically detect the presence in or intrusion or its attempt of intrusion to the controlled rooms or areas, to receive a manual emergency signal or to display such a signal.

Access control system: a system providing control of access into the given area. Its operation can be automatically or via a controlled manner.

Access point: the specific location, where access control takes place. The tool of control can be a door, a turnstile, a bar, etc.

Biometric identifier: such a device, which identifies a person based on a personal biological attribute (fingerprint, hand geometry, iris, face, etc.).

Unacceptable radiological consequence: a consequence of sabotage directed against a nuclear facility, nuclear material, a radioactive source or radioactive waste is unacceptable if it cause or might cause nuclear emergency. Furthermore, if the sabotage causes substantial exceedance of the dose limits for individuals or group of individuals in a short period or it is suitable to cause such extra radiation exposure.

Authority: Hungarian Atomic Energy Authority and National Police Headquarters.

Surface protection: or with other words shell protection basically includes the tools providing the security of the fence, boundary walls, floors, doors and windows.

Minimum (intrusion) warning system: surface protection extends over the doors and windows lower than 3 m, trap-like area protection is established, but there is no area, object or personal protection.

Partial (intrusion) warning system: in this case the surface protection is full scope (the warning system controls all such doors and windows, portals and walls, floors and banks that do not satisfy the requirements for full scope mechanical-physical protection and that are located at the perimeter of the protected object and it warns of any penetration or intrusion attempt through these), the area protection is trap like (the warning system monitors the access routes towards threatened objects and important areas within the facility), or the alarm take place on the scene (by alarming the direct vicinity).

Object protection: is meant to provide direct protection of the objects inside the rooms.

Full scope (intrusion) warning system: regarding surface protection the warning system controls all such doors and windows, portals and walls, floors and banks that do not satisfy the requirements for full scope mechanical-physical protection and that are located at the perimeter of the protected object and it warns of any penetration or intrusion attempt through these. Regarding area protection the warning system controls the interior area of the protected object, warns if each unauthorized human motion and, at least trap like manner, monitors the access routes. Regarding object protection the warning system controls all threatened objects. In personal protection the warning system continuously provide for all threatened persons the warning of potential attacks and, in addition to the local warning, the alarm initiated by the warning system directly warns the personnel tasked with the protection and guarding of the object.

Area protection: serves the security of interior rooms.

3. RECOMMENDATIONS OF THE GUIDELINE

In a complex security relation it is generally true that the electronic warning systems compensate for the potential failures due to surmountable mechanical protection and human mistakes and so they assume more and more role in physical protection. Their application needs less living force to carry out the same protection task and the expenses of mechanical protection can also be reduced. These systems require a single but larger investment, but their refund is proven on the long term.

The first step of establishment and design of the technical protection system as part of the whole physical protection system is the description of the environment. The preliminaries should be provided therein, such as: if the given facility will be new or will be a modification of an existing one of other function. It is necessary to determine the reason why the establishment or modification of the protection system is required.

It is extremely important to examine the location of the buildings: buildings of what purpose surround the given object or what traffic takes place within the surrounding area. It can be generally determined that nuclear facilities are located in less busy places, which is less favourable from the aspect of access, but it is simpler to recognize a potential illegal behaviour.

Structural description should include the characterization of walls, floors, roof structures, doors and windows, which are of importance to determine the type and number of sensors. The separation of various structures may also significantly influence the selection of the appropriate tools.

External disturbing factors should also be revealed during the survey, since future failures of the systems may also be traced back to that. Disturbing factors can be crossing high voltage transmission lines, high power radio transmitters, rebroadcasting stations, repeater antennas, air corridors, truck or underground traffic. Even information on sunshine (hours, distribution within the day, orientation of windows according to cardinal direction, or simply: sunshine penetrates from which direction, through which window, when and for how long).

3.1. General considerations

Nuclear facilities, nuclear and other radioactive materials (including transports or locations for final disposal of such materials) can be potential targets of adversaries. Such protection system should be developed to secure them, which is at all times commensurate with the threat level, so it provides adequate response if necessary, can be flexibly modified, expanded, developed and represents such a technical level, sabotage of which would require substantial professional skills.

Systems of detection physical protection function are as follows:

- Intrusion warning system,
- Video surveillance system, and
- Access control system.

The systems, structures and components of the detection physical protection function are classified to levels in harmony with the protection levels (A, B, C, D)

3.1.1. Intrusion warning system

Tools used for exterior protection are located outside the protected object. Shell protection basically involves the tools providing protection for fences, boundary walls, roofs, doors and windows. Area protection serves the security of internal and external areas. Object protection provides direct security for individual items in various rooms. In addition, the tools for personal protection are used for security of personnel and others, for example visitors. It is important to provide that the signals emitted by the warning system are detected by the personnel responsible for the security, surveillance and protection of the given object.

(1) The physical protection level A is equivalent with the full scope warning system. The system shall consist of the surface (shell), area, object and person protection. Within the protection the following shall be applied:

a) surface protection by the appropriate combination of
   - opening-,
   - glass breaking-, glass cutting-,
   - wall dismantling sensors, and
   - barriers;

b) area protection by
   - motion sensor;

c) object protection by the appropriate combination of:
   - vibration-,
   - metal sound-,
   - stressing-,
   - displacement-,
   - dismantling sensors, and
   - object traps; and

d) person protection by the appropriate combination of:
   - attack-,
   - vigilance-, and
   - leaning sensors.

(2) The physical protection level B and C is equivalent with the partial warning system. The system shall consist of the surface and area protection. Within the protection the following shall be applied:

a) surface protection by the appropriate combination of
   - opening-,
   - glass breaking-, glass cutting-,
   - wall dismantling sensors, and
   - barriers;

b) area protection
   - motion sensor.

3.1.2. Video surveillance system

The function of the video surveillance system or Closed Circuit Television (CCTV) is to monitor the events in interior or exterior areas. Its special advantage is that the visual information is recorded and analyzed and the incidents can be reconstructed subsequently.

(1) At physical protection level A, the video surveillance and assessment system shall consist of the following elements:

- digital (IP-based) cameras,
- optical image transmission devices, and
- plasma and LCD displays (monitors).

Furthermore, depending on the application, of the following:

- digital (IP-based) recorders, and
- infra reflectors, as supplements.

(2) At physical protection level B, the video surveillance and assessment system shall consist of the following elements:

- digital (IP-based) cameras,
- bunched conductor pairs and optical image transmission devices, and
- plasma and LCD displays (monitors).

Furthermore, depending on the application, of the following:

- digital (IP-based) recorders, and
- infra reflectors, as supplements.

(3) At physical protection level C, the video surveillance and assessment system shall consist of the following elements:

- analogue and digital (IP-based) cameras,
- coaxial and bunched conductor pairs,
- optical and wireless image transmission devices, and
- monitors.

Furthermore, depending on the application, of the following:

- analog and digital (IP-based) recorders, and
- infra reflectors. as supplements.

The application of video surveillance system is not mandatory in the case of level-D protection.

3.1.3. Access control system

Basically the access control systems control, monitor and document the movement into, out of and within the protected object across the entrance and exit points. It is required for the system to be able to prevent and/or warn such passes or access attempts, which are carried out by such persons who are not authorized to enter into or move within the object.

(1) At physical protection level A, the entrance control system shall consist of the following elements:

- security examination instruments, especially package examiner, explosion detector, metal detector and radiation gate,
- reading-verifying units,
- biometric identifiers, and
- access/egress points.

(2) At physical protection level B, the entrance control system shall consist of the following elements:

- reading-verifying units,
- personal identification elements, and
- access/regress points.

(3) At physical protection level D, the entrance control system shall consist of the following elements:

- lockable doors, and
- limitation of entrance rights.

The tables of below pages contain the classification of systems, structures and components applied for detection.

3.2. Specific recommendations

Components of the particular systems and the respective minimum requirements for their technical, physical characteristics are described below.

3.2.1. Components of the intrusion detector system

Opening sensors:

Tools of surface (shell) protection, applied to monitor doors and windows. By means of opening sensors it should be determined if the given door or window is open or close. REED relay solutions can be applied only for A-D-level intrusion detection systems, while mechanical sensors can be used only in Level-A intrusion detection systems.

Glass breaking sensors:

They are tools of surface protection. The glass breaking sensors are to provide the protection for glass windows or glass doors installed at the perimeter of the buildings. The tools can be divided into two groups: so-called glued sensors fixed directly onto the glass surface or acoustic sensors situated in the vicinity of the glass. Acoustic sensors can be used in any A-D-level, while the glued ones can only be applied in A-B level solutions.

Wall dismantling sensors:

They are tools of surface (shell) protection. The wall dismantling sensors can be metal meshes fixed onto the wall surface, body noise sensors containing piezo slices, or sensor cables placed under the ground (walking layers). Each type can be applied depending on the task to fulfill at any protection level (A-D-level).

Bars:

They are tools of surface (shell) protection. Bars can be used to close longitudinal areas, roads either in exterior or interior areas. Such tool contains a separate or jointly installed emitter and a receiver unit. It can be infra or laser ray operated. Each can be used for each protection level depending on the task to be solved (A-D-level)

Motion sensors:

Motion sensors are the tools of area protection, which are meant to detect the motion of unauthorized persons entering the protected area and transfers the signals induced thereby towards the intrusion detector centre. The dual (twin element) or combined motion detectors can be used for A-C-level, while passive infra (PIR) tools can be used for level-C protection. It is not required to apply motion detectors for level-D protection.

Vibration sensors:

They are tools of object protection. The vibration sensors detect physical impacts, especially hits affecting solids. According to their operation they can be mechanical or induction type vibration sensors. It is mandatory to use them exclusively for level-A systems.

Metal sound sensors:

They are tools of object protection; simplified versions of body noise detectors, usually to detect the noise of boring. It is mandatory to use them only for level-A systems.

Stress sensors:

They are tools of object protection. By means of prizing sensors the doors and windows can be protected against prizing. According to form of appearance they can be micro-switches mounted behind the click or piezo element. It is mandatory to use them exclusively for level-A systems.

Displacement sensors:

They are tools of object protection. They are meant to protect an object against displacement. They are always individual solutions fitting the character of the object. The object can be protected by a sensor installed in a holder or in the bottom or the back of the object, or even an opening switch can be used. It is mandatory to use them exclusively for level-A systems.

Object traps:

They are tools of object protection, being mechanical or optical type. In the case of mechanically operated type the object is fixed to a clamp. In the case of optical trap the object is placed on a light detector. If the object is removed a warning signal is generated after a pre-determined duration. It is mandatory to use them exclusively for level-A systems.

Attack detectors:

They are the tools of personal protection; an attack detector can be either installed in a fixed manner or used as a mobile tool. By means of them the person in trouble can request help without being noticed to doing so. Regarding the operation a contact switch is opened or closed. It is mandatory to use them exclusively for level-A systems.

Vigilance detectors:

They are the tools of personal protection. A tool, such as a pedal should be operated or a password should be entered with a defined frequency. Their task is to prevent the person from deviate his/her attention or to decrease his/her awareness. It is mandatory to use them exclusively for level-A systems.

Leaning sensors:

They are the tools of personal protection. The leaning sensor gives signal if the person leans. Usually it is an inertia switch, which establishes a contact if an angle from the horizontal is detected or in more modern instruments the electronic devices equipped with gyroscope decides the alarm generation based on preprogrammed parameters. Movement or necessary running of the protected person deviant from the natural should be taken into account in the design. The device should be connected directly to a radio (this can be the service radio at the same time). It is mandatory to use them exclusively for level-A systems.

3.2.2. Components of the video surveillance system

Image sensors (cameras)

Minimum requirements for image sensors (cameras):

Requirement	Level-A	Level-B	Level-C
Resolution (TV row)	480	400	320
Signal/noise ration (dB)	50	48	45
Digital signal processing	yes	yes	not mandatory
White balance *	yes	yes	not mandatory
Nigh/day switch *	yes		
Packet switching data transmission	yes	yes	not mandatory
- Frames per second (fps)	24	20	15
- Data transmission encryption	yes	yes	not mandatory
- Camera access	password protected		

*: only in the case of color image sensors

Digital image sensors (cameras) can be used in each of the levels A, B and C, while analogous devices can be used only in level-C and level-D.

Image transmission devices*:*

During the construction of the video surveillance systems, when using fiber optic cables, it should be taken into account that the loss values allow at least 3 cable extensions or repairs throughout the lifetime of the system. Span wire should not be applied. Optical cable can be used in level A, B and C, while coaxial cable and wireless image transmission is allowed only in level-C systems.

***Image displays (monitors)**:*

Minimum requirements to be satisfied by image displays (monitors):

Requirement	Level-A	Level-B	Level-C
Resolution (pixel)	1920 x 1080	1280 x 1024	1024 x 768
Contrast ration	15000 : 1	8000 : 1	5000 : 1
Illuminance (cd / m^2)	500	500	350

Only plasma and LCD/LED image displays (monitors) should be applied in protection level A, B and C.

Image recorders:

Minimum requirements to be satisfied by image recorders:

Requirement	Level-A	Level-B	Level-C
Maskable motion detection	yes	yes	not mandatory
Recording and display during playback	yes	yes	not mandatory
Movable camera control	yes	yes	not mandatory
Preservation of image data secrecy	yes	yes	not mandatory
Connection to LAN network	yes	yes	not mandatory
Authenticity of recorded material (digital authentication)	yes	not mandatory	not mandatory
Alert output (by camera)	1	4	8
Resolution during recording and display (CIF)	4	2	1
Recording speed (fps /camera)	25	20	15

Beyond that, the following requirements are valid for all levels:

a) A warning signal should be generated and the assigned camera image should be displayed in full screen and in a secondary monitor output for a pre-set

time if a signal is received on the alarm input or if the installed video motion detector warns.

b) Continuous recording, separate recording of the alarm and the combination of them should be possible.

c) Split screen mode and full screen mode should be supported.

d) Step play back image display should be possible on every monitor output.

e) The cameras should have text identifiers and these identifiers should be displayed on the recorded images.

f) The recorded and transmitted images should be provided with time and date stamp.

g) The units should be able to notify the loss of video signal by channels.

h) Recorded images should not be lost if power supply is interrupted. The last mode before the loss of power supply should be returned after recovery.

i) Only the authorized user interface should be available after switch on.

j) Appropriate archiving tools should be available to archive the necessary image data.

k) The name of the camera should be assigned to the image during recording.

l) Protection against unauthorized modification of the program.

Only digital (and/or IP) recorder can be applied in protection level A, B and C.

3.2.3. Components of the access control system

Security checking tools:

- Luggage scanner. Usually X-ray equipment. It can be mobile of fixed. It should be able to scan at least 5 mm metal. The particular volume element should be possible to be scanned from above and side. Image processor should support the work of the operator.
- Explosive detector. Usually Ionmobility Spectrometers (IMS). In addition to detection of explosives, the dual systems (DIMS) should be able detect narcotic drugs. They can be programmed for at least 20 materials, the maximum detection time is 10 s. Detection limit for drugs depending on the type of the drug (cocaine, heroin, LSD etc.) is 1-5 ng, while for explosives (TNT, RDX, PETN, Semtex etc.) it should be 50-200 pg. The sampling tool is usually uses vacuum.

- Metal detector. They should be able to detect metals, metal alloys and non-magnetic steels. It can be fixed (metal detector gate) or manual. It should be resistant to electromagnetic interference and it should be operable near to strongly reinforced floors. Detection level of metal detector gate should be high even if high a passing speed (max. 5 m/s).
- Radiation screening gate. Fixed, high sensitivity detector systems should be used for detecting hidden (disguised) radioactive materials. Its technical parameters should be specified based on the probability of occurrence of detection events at the location of installation.

Their application is mandatory for level-A protection.

Reader terminal:

a) It should be able to recognize the identification code system applied in the particular access control system and to transmit the identification code towards the control unit.

b) Removal of the terminal from its location of installation, opening of its housing should be possible only by specific tools.

c) Hidden or monitored cable connections should be available against external manipulation.

Control unit:

a) It should control the structures inhibiting the passing by at the access points and monitor the security status of the access point (closed, open, unauthorized opening, too long opening, sabotage, emergency opening).

b) It should initiate alarm for unauthorized opening of the access point.

c) It should initiate sabotage alarm if the protected units are opened.

d) Post-checking of set control values and process parameters should be possible.

e) Break of the communication of the controls in the common network and/or with the control centre or the reconnection should not cause or make the unauthorized access possible.

f) Removal of the unit from its location of installation, opening of its housing should be possible only by specific tools.

g) The housing should be provided with sabotage protection against opening.

Central unit:

a) Parameters of the hardware elements of the central unit should satisfy the requirements by the applied software and the connected data network and should ensure the continuous operation (7 x 24 hours).

b) Only that software should run on the central unit which is necessary for the operation of the access system.

c) An interface card should be connected and should handle the same number of controlled outputs and loop inputs as the number of handled control units. An event printer should be available that is able to perform real time printing, if necessary.

d) Uninterruptable power supply should ensure the operability in the case of loss of power supply for 8 hours.

e) It should automatically launch the access control software after switch on, the log off from which should be possible only by the system administrator.

Access card:

Proximity and chip cards can be applied. It is recommended to place security improving elements on the cards: photo, embossed print, laser engraving, hologram, etc. The use in combination with a code is also practical. They can be applied for protection level B, C and D.

Elements of passing points:

a) Doors. The doors can be traditional, simple doors, but control of passing can be implemented by means of turnstiles or locks. As an accessory element magnetic lock, electric lock and planar adhesive magnet etc.

b) Bars. Swing bars, three or more leg turnstile bars, splitting bars can be used. During the design of passing capacity the type of the bar to be used at the particular location should be taken into account.

They can be used for each protection level (A-D).

Minimum requirements to be satisfied by access control points:

Requirement	Level-A	Level-B	Level-C	Level-D
Management of access validity	yes	yes	yes	no
Log keeping	yes	yes	no	no
Control of open-close state	yes	yes	no	no
Number of codes (minimum)	10^6	10^5	10^4	10^3
Percent of invalid acceptance (%)	≤ 0.01	≤ 0.01	≤ 0.01	-

3.3. Other recommendations

Guarantee provision:

Minimum for the detection physical protection systems and components:

The contractor should guarantee the systems and components:

a) in the case of level-A systems: for 12 month + 48 month,

b) in the case of level-B systems: for 12 month + 24 month,

c) in the case of level-C systems: for 12 month + 12 month,

d) in the case of level-D systems: for 12 month.