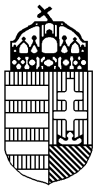
Hungarian Atomic Energy Authority



Guideline PP-14

Operation, maintenance and testing of physical protection systems and components

Version:

1.

Approved by

_____

Dr. József Rónaky

director-general

Hungarian Atomic Energy Authority

Budapest
2011

Published by: Dr. József Rónaky, director-general of HAEA
Budapest, 2011 October

The publication can be purchased from:
Hungarian Atomic Energy Authority
Budapest

PREAMBLE

The legal hierarchy of security regulations for nuclear facilities, nuclear and other radioactive materials is as follows:

1. The internationally accepted basis of physical protection is represented by the Law Decree 8 of 1987, which promulgated the Convention on Physical Protection of Nuclear Materials approved by the IAEA in 1979 and by the Act LXII of 2008, which promulgated the Modification of the Convention signed on July 8, 2005 in a diplomatic conference organized by the IAEA.

2. The uppermost level of domestic application of the obligations undertaken in the international convention is represented by the Act CXVI of 1996 on Atomic Energy (hereinafter referred to as: Atomic Act). The Atomic Act contains the basic concepts of nuclear security and establishes the basis for detailed regulation of physical protection.

3. Govt. Decree 190/2011. (IX. 19.) Korm. on physical protection requirements for various applications of atomic energy and the corresponding system of licensing, reporting and inspection issued as an executive order of Paragraphs q) and r) of Section 67 of the Atomic Act is the next level of the regulation system.

4. The methods how the requirements determined in the laws should be complied with are described in the *guidelines* that constitute the next level of the regulatory system. The guidelines are issued by the director general of the HAEA, and they are regularly reviewed and reissued based on accumulated experience. So as to proceed smoothly and duly the authority encourages the licensees to take into account the recommendations of the guidelines to the extent possible.

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.haea.gov.hu.

TABBLE OF CONTENTS

1. INTRODUCTION

1.1. Scope and objective

The guideline contains recommendations on how to meet the provisions of Govt. Decree 190/2011. (IX. 19.) Korm. (hereinafter referred to as: Govt. decree) on physical protection requirements for various applications of atomic energy and the corresponding system of licensing, reporting and inspection.

This guideline provides detailed guidance and practical example on how to comply with the requirements on operation, maintenance and testing of the physical protection systems and components to facilitate the compliance therewith.

1.2. Corresponding laws and regulations

- Act CXVI of 1996 on Atomic Energy
- Govt. Decree 190/2011. (IX. 19.) Korm. on physical protection requirements for various applications of atomic energy and the corresponding system of licensing, reporting and inspection.

2. DEFINITIONS

Authority: Hungarian Atomic Energy Authority and National Police Headquarters.

Nuclear security: set of such activities, tools and procedures, which are directed to prevent and detect of, response to and manage the consequences of sabotage or a malicious act or unauthorized removal related to nuclear or other radioactive material or a nuclear facility.

Threat: hazard or act threatening the peaceful users of atomic energy determined by the state in an updated threat assessment.

Design Basis Threat: such level of threat determined by the state, against which the user of atomic energy shall provide effective physical protection.

Physical Protection: the complex set of those internal regulations, technical equipment and live response forces, which are applied as part of nuclear security for deterrence, detection and delay of and response to unauthorized removal and sabotage committed against nuclear facilities, nuclear and other radioactive materials.

Physical protection plan: a plan describing how physical protection system functions and how the deterrence, detection, delay and response physical protection functions are implemented.

Sabotage: Any deliberate act directed against a nuclear facility, nuclear or other radioactive materials, interim storage facility and final repository of radioactive wastes or any system, structures or component important from the aspect of radiological consequences, which may cause public threat (Section 259 of Penal Code), interference with the functioning of facilities of public concern (Section 260), damaging of environment (Section 280) or the attempt or preparation thereof.

Causing public danger and damaging to the environment with the use of nuclear and other radioactive materials: causing of public danger (Section 259) and damaging to the environment (Section 280) committed intentionally with nuclear and other radioactive materials or the attempt thereof according to the Criminal Code.

Unauthorized removal of nuclear or other radioactive materials: theft (Section 316) or robbery (Section 321) of nuclear or other radioactive materials according to the Criminal Code.

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.

Obligant: licensee of a nuclear installation, interim radioactive waste storage or final radioactive waste repository, holder of a radioactive source, holder of radioactive waste and holder of nuclear material.

Audit: review of reports. It usually relates to an operating system, process or product and reviews how it complies with the expectations, requirements. The audit is part of the quality

assurance audits, and can be a tool to qualify the organization according to a standard. It can be performed by internal (member of the organization) or external auditor.

Internal audit: the organization itself performs the audit or is performed at its request for internal purposes. For example the implementation of such an audit can be taken as basis to issue a Statement of Compliance or to state about a specific system that it complies with the regulations, requirements.

3. RECOMMENDATIONS

3.1. General considerations

In relation to operation, maintenance and testing the question, which has to be always answered is whether the physical protection system(s) and the respective system components are in compliance with the expectations and requirements from all aspect. The compliance can be demonstrated through the implementation of a series of specific inspections (audit), which covers the entire complexity of the correlated systems.

The correct operation of the physical protection systems and system components is usually overseen by everyday witnessing of their activities and in the lack of error messages or obvious failure, if their operation is continuous except for the maintenance periods.

Normal maintenance takes place in the frame of measures of the given protection regime with a specified frequency, while tests are usually run by the electronic systems automatically. Beyond that it is also necessary to periodically and comprehensively inspect the systems, system components with the aim of auditing if the complex physical protection is in compliance with the relevant requirements. If this is done by the operating organization or by external professionals for internal purposes, then the audit is internal.

Internal audits should be performed with a frequency defined in the standards, regulations or in the quality management system. If any non-compliance, failure, damage or other severe deficiency occurs, then the management should order an immediate extraordinary audit. It is practical that the manager responsible for the area to be audited invites professional(s) independent of the given area or external professional(s) to perform the audit.

The security manager or the manager assigned for the given area should be responsible for the internal audit and to plan and implement all the related operative activities.

The results of the internal audits, the decided corrective actions and their review should be documented.

3.2. Specific recommendations

3.2.1. Audit of safety and security related areas

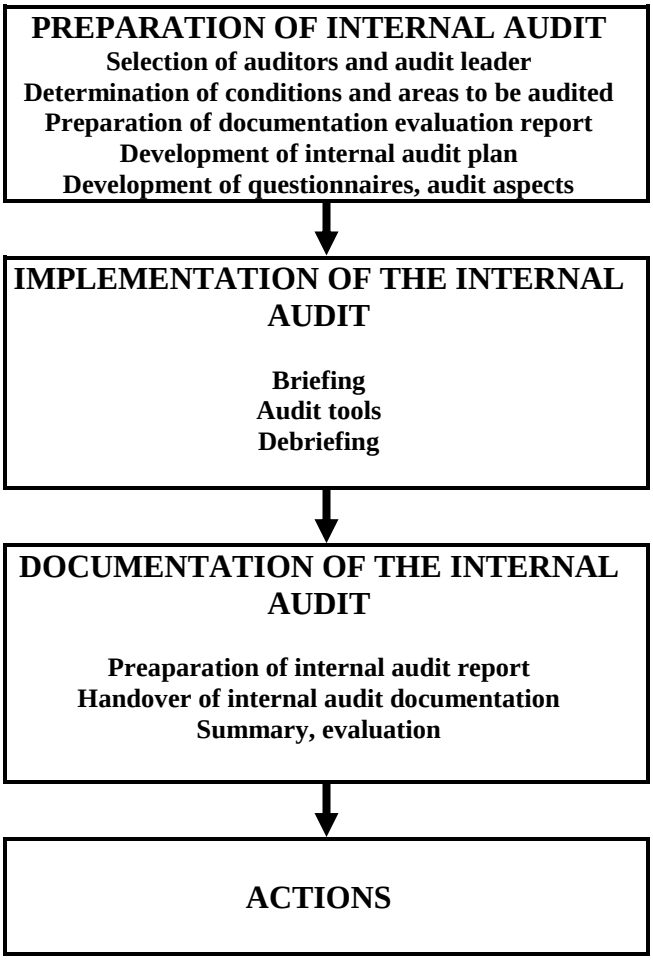
Security audits usually take place in the following areas:

- security techniques and security of property (set of mechanical, electronic, living force regime measures),
- work protection,
- fire protection,
- information security,
- human security,
- crisis management.

Since the elements of safety and security strategy belong to various areas, therefore their joint operation should be verified and controlled all the time.

3.2.2. Internal audit process of the physical protection systems

General process of audits to be applied is displayed in the figure below:



3.2.3. Preparation of internal audit

3.2.3.1. Selection of auditor(s) and audit leader

The most effective way to carry out an internal audit is an inspection with the involvement of external professional(s) (in order to most effectively implement the audit it is possible to involve more professionals).

Experts with due professional background and experience in the given area should be invited to carry out the audit. The references requested should always be verified and the information obtained should be evaluated.

3.2.3.2. Determination of the conditions and areas to be audited

The following items should be determined:

- areas and processes to be audited,
- audit tools and the respective authorizations (scope of competence of the auditor during the reviews),
- order of handing over of the documentation,

- schedule (deadlines),
- content of Confidentiality Undertaking,
- order of data and documentation management (what documents can be requested from the various areas and how these should be managed, stored etc.),
- content of Credentials.

3.2.3.3. Preparation of documentation evaluation report

Based on the documentation provided to the auditor, he/she should prepare for the audit. The comments made during review should be recorded in the Documentation evaluation report. Based on the report the auditor should decide whether the audit might take place or not.

3.2.3.4. Development of internal audit plan

Prior to the commencement of the reviews the concerned personnel should be informed (the audit should not interfere with the work process or the organization). The Customer of the audit should inform the managers of the areas to be audited about the audit in a circular.

3.2.3.5. Development of questionnaires, audit aspects

Based on the requested documentation the auditor learns the safety and security concept, security instructions and system of requirements of the Customer. His/her own professional aspects should be developed based on this information by weighing the particular potential failures and positive results (in the area of physical protection almost all kind of failures might entail downgrading, since it is an activity of high risk). The questionnaires, forms are integral parts of the audit (the evaluation table, diagrams should be prepared based on them).

3.2.3.6. General outline of the questionnaires and forms of the physical protection system audit

The questionnaires prepared for the audit processes may be different from each other depending on the area to be reviewed.

General content of the audit on mechanical elements:

- Data (location, date, accompanying person etc.),
- Type and state of external protection (fences, bars, buildings, doors, grills etc),
- Type and state of internal protection,
- Documentation (existence, actuality, management),
- Comments, recommendations,
- Summary of points.

General content of the audit on electric elements:

- Data (location, date, accompanying person etc.),

- General survey (verification of management and state of security system etc.),
- System description (state and use of intrusion alert, video survey, entry system or respective measures),
- Qualification of installation (compliance with laws, standards and requirements),
- Operability of the system,
- Inspection of the auxiliary tools influencing the system (lighting, backup units, uninterrupted power supply etc.),
- Documentation (existence, actuality, management),
- Implementation of maintenance and existence of the respective documentation,
- Comments, recommendations,
- Summary of points.

3.2.4. Implementation of the internal audit

3.2.4.1. Briefing

The participants of the briefing are the manager of the area (process or activity) to be audited and the personnel designated by him/her, the audit leader and the auditor. During the briefing the auditor describes the goals, scope and schedule of the audit and finalizes the sequence of review steps.

3.2.4.2. Audit tools

The audit process can be implemented by following open, operative or provocative methods or the combination of these.

Open inspection method (observer status):

It is implemented at a predetermined date, with predefined questions and designated person(s) (standard audit procedure which can be applied as requested by the customer).

Operative inspection method (observer status):

The audit date, the auditor and the questionnaire are not know in advance, but the area and activity to be audited is known. It involves, according to the preliminary permits, observations, taking of photos, background analyses and preparation of records. This procedure is primarily applied to internal audits, which can be carried out by the security manager, his/her agent or an external professional. Immediate recording of an error by the possible involvement of the concerned staff can be an operative audit.

Provocative inspection method (intervention role):

Intentional violation of a process, causing of failure, generation of extraordinary situations, creation of unusual circumstances.

3.2.4.3. Debriefing

Subsequent to the termination of the audit the auditor holds a debriefing with the managers of the areas audited or with their designated personnel, the purpose of which is to describe and make them understand the results and statements of the audit. The auditor should describe the statements of the audit according to their importance and the final conclusions reflecting the goals set for the audit. The auditor should provide recommendations with deadlines for the elimination of the non-compliances.

3.2.5. Documentation of internal audits

3.2.5.1. Preparation of internal audit report:

Based on the filled questionnaires, records, summaries and evaluations the auditor compiles the audit report together with the audit leader. This should contain all explored results, data, comment, etc.

3.2.5.2. Handover of documentation of internal audit:

The documentation of the internal audit consists of the following:

- Credentials;
- Internal audit plan;
- Documentation evaluation report;
- Internal audit report;
- Internal audit records;
- Records of non-compliances;
- Questionnaires;
- Records;
- Photos, other collected materials.

3.2.5.3. Summary, evaluation:

The summary shall contain:

- The areas of the audit;
- Location, identifier and time of sampling;
- Method of inspection;
- Description of particular and important examples.

After the implementation of the audit, based on the information collected, the areas reviewed should be evaluated and commented. Specific suggestions should be formulated beyond the general “compliant” or “non-compliant” qualification.

3.2.6. Actions

Corrective actions should be implemented by the persons responsible for the given area when all the facts are collected.

3.2.7. Audit of the mechanical protection

During the audit of instruments of mechanical protection the area and space separators are inspected, as well as the state, effectiveness and quality of doors, locks and padlocks and their professional assembly.

3.2.7.1. Open inspection method

- Locks, padlocks, other locking means,
- Fence lines,
- Doors, sluices, fire doors, space separators,
- Quality, reliability and effectiveness of security grills, foils, shutters,
- Location and effectiveness of physical objects, devices to impede an attack,
- Method, effectiveness, documentation of key management, update of sample signatures, etc.,
- Knowledge of requirements for the use of tools and objects.

3.2.7.2. Operative inspection method

Implementation of all the inspections listed above in a manner not unconditionally extended over every area, with preliminary not known question list and at a random date, to inspect

- Use of forbidden areas;
- Locking of compartments and routes.

3.2.7.3. Provocative inspection method

- Detection of extraordinary events, change of physical conditions;
- Inspection of operability of systems and tools when an extraordinary event occurs;
- Generation of mandatory key management failures, etc.

3.2.8. Audit of electronic protection

The audit should verify the operability, state and effectiveness of systems, tools and accessories and if the installation is carried out in a professional manner. The audit extends over the use of tools, documentation of training records and knowledge of training material.

3.2.8.1. Open inspection method

- Quality, reliability, operability and effectiveness of installed systems;
- If the installations are in compliance with standards, requirements or possible with the order;
- Existence, management and updating of access codes;
- Realization of systems maintenances;
- Inspection of documentation (maintenance records, worksheets, system descriptions etc.);
- Knowledge of requirements for use of tools and objects.

3.2.8.2. Operative inspection method

Implementation of all the inspections listed above in a manner not unconditionally extended over every area, with a question list not known in advance and at a random date, and

- Run of system tests and verification of settings during out of active periods,
- Verification of knowledge how to operate the tools.

3.2.8.3. Provocative inspection method

- Detection of extraordinary events, change of physical state;
- Observation of operability of systems and tools when extraordinary events occur, etc.