Hungarian Atomic Energy Authority

(This is an unofficial translation of the text)

PP-18 Guideline

Protection requirements for computer systems

Version:

2.

2016 February

Published by

Gyula Fichtinger

Director General of the HAEA

Budapest, 2016

The publication is available:

Hungarian Atomic Energy Authority

Budapest

Országos Atomenergia Hivatal

DIRECTOR GENERAL FOREWORD

The Hungarian Atomic Energy Authority (hereinafter referred to as: HAEA) is a central state administration body with national competence in the field of peaceful use of nuclear energy. The HAEA was founded by the Government of the Republic of Hungary in 1990.

The public function of the HAEA as defined by law, is independent of the organizations involved in the application of atomic energy, support and coordinate the regulatory activities related to the peaceful, safe and secure application of atomic energy, including nuclear and radioactive waste facilities, the safety of nuclear and other radioactive materials, nuclear emergency management, nuclear safeguards, as well as the public information tasks related to these, furthermore to propose legislation for the application of atomic energy, to modify and to preliminary opinion on legislation related to the application of atomic energy.

The fundamental objective of the regulatory oversight of the use of atomic energy is that the peaceful use of atomic energy cannot in any way cause harm to persons or the environment, but the authority does not to a greater than justified extent limit the operation of the facilities or the pursuit of their activities. The fundamental safety objective applies to all installations and activities, and to all phases of the lifecycle of a facility or radioactive source, including design, siting, commissioning and operation, and decommissioning, shut down and closure, in the case of repository of radioactive waste the post-closure period, in the case of the application of nuclear materials the transportation related to their application and the management of radioactive waste, while in the case of equipment emitting ionizing radiation their operation and maintenance.

The HAEA outlines the way in which regulatory requirements are met, in consultation with the users of atomic energy in Guidelines that contain clear, unambiguous recommendations, which are sent to stakeholders and made accessible to all members of the society. Guidelines on meeting nuclear safety, radiation protection and non-proliferation requirements related to the use of atomic energy are published by the Director General of the HAEA.

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.

PREAMBLE

The internationally accepted basis for 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, as well as by Act XX of 2007 on the promulgation of the International Convention for the Suppression of Acts of Nuclear Terrorism.

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.

Based on the authorization provided in the Atomic Act, 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 (hereinafter referred to as: Decree) contains detailed legal requirements.

To comply with the statutory requirements, the HAEA may formulate recommendations, which will be issued in the form of Guidelines and published on the HAEA website. This Guideline applies voluntarily to licensees and does not contain generally mandatory norms. 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.

When using methods other than those described in the Guidelines, the HAEA examines the correctness, appropriateness and completeness of the method used, which can result in longer administration times, may involve external experts and additional costs. If the method chosen by the licensee differs from the one recommended by the Guideline, the deviation must be justified.

The Guidelines are reviewed at intervals specified by the HAEA or at the suggestion of the licensee.

The above regulations are supplemented by licensees and other internal regulatory documents of organizations involved in the application of nuclear energy (designers, manufacturers etc.) that are prepared in accordance with their control systems.

TABLE OF CONTENS

1. INTRODUCTION

1.1. Scope and objective

Given that programmable systems play an important role in the context of peaceful uses, safety and security and that the personnel involved in the implementation of the guideline are identical, this Guideline is special in the sense that its scope covers programmable systems related to peaceful applications, nuclear safety (including technical radiation protection) and nuclear security, as well as its aim is to provide regulatory guidance on the handling of unintentional or intentional threats. Accordingly, the Guideline discusses the systems concerned, the related requirements and recommendations together (this aim is represented by the term „protection requirements" in the title).

The guideline contains guidance on:

a) The security of the programmable control systems and components connected directly or through stored information to the technological systems under the effect of the Nuclear Safety Code (NSC) issued as Annex of the Govt. Decree 118/2011 (VII.11) Korm. on the nuclear safety requirements of nuclear facilities on related regulatory activities also contributes to nuclear safety;

b) the compliance of implementation of physical protection of computer and instrumentation and control systems under the effect of 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;

c) the compliance of ensuring the safety of record keeping and operating records, prevention of unauthorized access to data in accordance with Ministerial Decree 7/2007 (III. 6.) IRM (hereinafter referred to as: IRMr) on the rules of accountancy for and control of nuclear material;

d) the compliance of ensuring the safety and the prevention of unauthorized access to the data contained in the registers under the effect of Ministerial Decree 11/2010. (III. 4.) KHEM of the Minister of Transportation, Communication and Energy on the registration and control order of radioactive materials and related data supply.

The Guideline provides guidance on the requirements for the protection of programmable systems with nuclear safety functions (including technical radiation protection functions), physical protection functions, nuclear safeguards requirement fulfilment as well as radioactive material

accountancy functions against intentional or unintentional threats, and the content of the security plan of the programmable systems.

The guidance provided by the Guideline does not cover the general protection requirements of administration networks. The guidance addresses those portions of the administration networks, which have correspondence to a programmable system or component having a nuclear safety, physical protection, nuclear safeguards or radioactive material registration function. The Guideline does not contain guidance on general data protection issues.

The objective of the Guideline is to provide that such protection measures and a protection plan to the programmable systems are developed, which ensure at an acceptable level the designed operation mode of programmable systems and components in relation to

a) availability,

b) integrity and

c) confidentiality

of the data processed, stored or forwarded in programmable systems and components

a) connected to system components fulfilling nuclear safety (including technical radiation protection) function,

b) connected to system components fulfilling physical protection function,

c) connected to system components important from the aspect of operation of the facility,

d) connected to system components fulfilling nuclear safeguards requirements function,

e) connected to the registration of nuclear materials.

The recommended protection measures in addition to protecting against unintentional threats are also meant to ensure protection against the following malevolent threats:

a) information gathering for planning and execution of a later action;

b) obstruction or disturbance of operation of programmable systems and components essential for safe operation and physical protection of the facility.

The protection of programmable systems and components is a very quickly developing field and consequently the Guideline could not aim to

encourage particular protection measures, but instead of it, formulated general principles and methods.

1.2. Corresponding laws and regulations

Based on the empowerment given in Subsection 174/A (1) of Act CXL of 2004 on General Rules of Public Administration Procedures and Services and according to Section 67 of the Act CXVI on Atomic Energy the Government is empowered to regulate:

a) among others the nuclear safety requirements related to the design, manufacture, purchase, commissioning and modification of nuclear systems, structures and components and the requirements imposed on the quality assurance systems of organizations participating in such activities as specified in Para. d) of the Section;

b) tasks and obligations of atomic energy users and the competent authorities as specified by Para. c) of the Section;

c) the operation of bodies performing up-to-date threat analysis in relation to nuclear security and determining the design basis threat as specified by Para. q) of the Section;

d) the physical protection requirements and the related authority system and procedures in relation to the use of atomic energy as specified by Para. r) of the Section.

The requirements for which written recommendations are provided in this Guideline are included in the following laws:

- Govt. Decree 118/2011 (VII.11) Korm. on the nuclear safety requirements of nuclear facilities and the corresponding regulatory activities and the Nuclear Safety Code issued as Annexes to the decree,
- Govt. Decree 190/2011 (IX. 19) Korm. on physical protection requirements for various applications of atomic energy and the corresponding systems of licensing, reporting and inspection,
- Ministerial Decree 7/2007 (III. 6.) IRM on the rules of accountancy for and control of nuclear material

The scope of the Guideline covers the protection requirements of programmable systems. Item 17a of Subsection (1) of Section 2 of Govt. Decree 190/2011 (IX. 19) Korm. on physical protection requirements for various applications of atomic energy and the corresponding systems of licensing, reporting and inspection, defines programmable systems:

17a. programmable system: a functional device or structure capable of performing computing, communication, automation, monitoring and control functions, including:

a) control engineering systems related to the facility's technology

b) physical protection systems;

c) safeguards systems,

d) radioactive material registering systems, and

e) those nuclear safety, physical protection, safeguards and radioactive material register systems not directly connected to the technology of the facility, the data or information stored and handled therein are under the responsibility of the licensee.

Based on Para. e) of the definition of programmable system, Govt. Decree 190/2011 (IX.19) Korm. shall be applied to all system components of the administration network where data, information related to nuclear safety, physical protection, nuclear safeguards and radioactive material accountancy systems are stored and managed.

In the case of the spent fuel interim storage facility, the protection of systems and system components under the effect of Volume 6, Chapter 6.2.4 of NSC shall be ensured.

Section 20 of the Govt. Decree 190/2011 (IX.19) Korm. prescribes the obligation of the licensee in relation to the protection of programmable systems:

a) ensure the confidentiality, integrity and availability of the managed data and information stored in the programmable systems, as well as the physical protection of the programmable system proportionally to the integrity and availability risks;
b) prepare a security plan describing the structure and operation of the programmable systems as part of the physical protection plan.
c) establish or designate an organizational unit directly under the supervision of the senior management of the facility to supervise the physical protection of the programmable systems;
d) the organizational unit established or designated consists of delegation of the organizational units involved in the physical protection of programmable systems and components or the employees of the designated organizational unit.
e) act on the basis of Annex 6 of the Decree during the design, construction and modification of the programmable systems.

In the case of an operational nuclear power plant the joint implementation of paragraphs 3.4.5.2000., 3.4.5.2100., 3.4.5.2400., 3.4.5.2700., 3.4.5.2800., 3.4.5.3100., 3.4.5.3200. and 3.4.5.3300 of Volume 3 of Chapter 3.4.5 of the NSC serves nuclear safety while at the same time supports nuclear security. Paragraphs 3.4.5.3500 – 3.4.5.4000 represent aspects of nuclear security, contributing to the realization of nuclear safety.

This regulation is well adjusted to the spirit of the Govt. Decree 190/2011 (IX.19) Korm.

3.4.5.2000. *The programmable systems and components shall be designed and implemented according to the standards selected to use for programmable systems and components according to graded requirements.*

The need to follow several such IEC standards concludes from this requirement, which has to take into account the *IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety - General requirements for systems* principal standard. The standards to be referred here are listed in Section 1.3.

The requirements below describe a very important IT constraint.

3.4.5.2100. The human and automatic interactions between the programmable systems and components and the outside world shall be determined in the form of logical and physical interfaces. The designed interactions shall not hinder the performance of automatic safety functions.

This requirement represents the principle that if the separation of the systems connected to the process equipment could not be provided, then such supplementary protections should be installed on these systems that are not compatible with the principles of the standard IEC61226, namely with the principle of deterministic operation in Category “A”, and with the principle of simplicity in Category “A” and “B”, which concludes to the principle that only such software components should be installed which serve exclusively process functions.

The third requirement describes a very important IT and physical protection requirement, especially in relation to access control systems.

3.4.5.3200. Suitable design solutions and measures shall ensure that the programmable systems and components can be accessed, both physically and logically, only by those persons for whom it is necessary and permitted to perform a specific task and at such a level and with such options that are necessary to perform the task.

The Guideline 3.5 for the NSC contains recommendation about the compliance with nuclear safety requirements related to programmable

systems and components connected to process equipment. This Guideline is meant to supplement these recommendations to comply with the physical protection requirements in such a way that it covers also the systems which are not under the effect of the nuclear safety regulations.

In the case of a new nuclear power plant, the combined management of nuclear safety and security consideration begins during design. The design requirements of new nuclear power plants are described in Chapter 3a.4.5 of Volume 3a of the NSC, including:

3a.4.5.1600; 3a.4.5.1800; 3a.4.5.2000; 3a.4.5.2100; 3a.4.5.2200;
3a.4.5.2400; 3a.4.5.2600 (independence); 3a.4.5.2700 d);
3a.4.5.2800. (response time); 3a.4.5.3100; 3a.4.5.3200 c), d) and e);
3a.4.5.3300; 3a.4.5.3400; 3a.4.5.3500; 3a.4.5.3600;
3a.4.5.4000. (failure tolerance and redundancy);
3a.4.5.4200 and 4300 (lower safety class subsystem shall not cause errors);
3a.4.5.4600. (manually initiated testing opportunity);
3a.4.5.4900 (full scope testing);
3a.4.5.5100 (certification);

describe such security requirements and subsequently system features that support the fulfilment of the requirements for the protection of programmable systems described in other legislation.

The following paragraphs of Chapter 3a of the NSC specifically serve nuclear security:

3a.4.5.3700 (no communication with a system outside the given unit, physically one-way communication channel)

3a.4.5.3800 (physically one-way communication channel)

3a.4.5.3900. (physically one-way communication channel, connection of diagnostic tools)

3a.4.5.4100. (defense in depth)

3a.4.5.4500 (self-check capability)

3a.4.5.4700 (minimization of common cause failures)

3a.4.5.5000 (access)

3a.4.5.5300 (Design Basis Threat and government decree on physical protection)

3a.3.6.2800. If there is a radio frequency or microwave electromagnetic radiation source with a significant energy density on or in the vicinity of the site, its effect on the systems and components important to nuclear safety shall be

assessed. If there is a possibility for such an effect, appropriate protective measures shall be provided.

3a.3.6.2900. The design basis hazard factors associated with human activities and their effects on systems, structures and components with safety functions shall be specified. Should these effects influence the performance of the safety function, protection against such effects shall be provided. The protection may also be provided through administrative tools, i.e. restricting human activities posing a hazard, but technical solutions for protection shall be preferred against these effects if such solutions can reasonably be accomplished.

3a.4.5.1400. Instrumentation suitable for the measurement of parameters necessary for monitoring fundamental safety functions shall be provided, thus ensuring the availability of information necessary for the reliable and safe operation of the nuclear power plant unit and the management of events resulting in TA2-4and TAK1 and TAK2 operating conditions.

3a.4.5.1900. Instrumentation and control systems shall be so designed that they can be simply refurbished even several times during the operating time of the unit. The refurbishment strategy to be applied for instrumentation and control systems during the operating time of the unit shall be described in the construction licence application.

3a.4.5.2200. Facilities subject to strict administrative monitoring shall be provided for changing systems or system components important to nuclear safety, their instrumentation and control configuration, operating logic or the data associated with them.

3a.4.5.3100. All data important to safety shall be archived. A time stamp shall also be attached to the data. The time stamp shall be generated the closest to its generation in the data stream, as early as possible. The archive shall be retained until the end of the operating time of the units.

3a.4.5.3700. The ABOS 2 systems and components shall not communicate with a system outside the given unit, and shall provide data to a system or component of the same unit in a lower safety class only via a physically one-way communication channel.

3a.4.5.3900. An instrumentation and control system connected to the technology shall provide data to the instrumentation and control system of another unit or to external systems only via a physically one-way data connection. An ABOS 2 system shall be connected to instrumentation and control systems in a lower class for the purpose of exporting data only via a physically one-way communication channel. In the case of diagnostic tools and equipment used for repair service purposes, it shall be demonstrated that the entry of inadvertent or malevolent commands in the safety system is excluded

from the direction of the connected diagnostic tools and equipment used for repair service purposes. In the case of ABOS 3 systems, it shall be demonstrated that the entry of inadvertent or malevolent commands is excluded from the direction of the connected systems and components included in lower classes.

3a.4.5.4000. The subsystems of the instrumentation and control systems in Safety Class ABOS 2 shall be redundant to an extent sufficient for the fulfilment of the required failure tolerance. The functionality of redundant stocks shall be as identical as possible while applying the intended diversity.

3a.4.5.4100. The architecture of the instrumentation and control systems shall fit into the levels of defence in depth. The levels fitting into defence in depth shall be separated from each other to the extent reasonably achievable.

3a.4.5.4200. Non-safety functions or functions assigned to lower functional safety levels shall not be integrated into a subsystem included in a safety class or in a safety class that is higher than necessary. If this is not possible, it shall be demonstrated by safety analysis that the subsystem performing a function in a lower safety class does not, in any way, hinder the performance of any function in a higher safety class.

3a.4.5.4300. In the case of connections between instrumentation and control systems included in different safety classes, it shall be demonstrated that the system in the lower class has no influence on the operation of the system in the higher class. In the case of connections between instrumentation and control systems in the same safety class, it shall be demonstrated that the failure of one of the systems does not hinder the performance of the automatic safety functions of the other.

3a.4.5.4700. In the case of instrumentation and control systems included in Safety Class ABOS 2, the potential for common cause failures shall be minimized by the application of functional or system component level diversity to the appropriate extent. The necessary extent of diversity shall be deduced from the required reliability requirements. It shall be verified by analysis that the probability of common cause failures is sufficiently low with the selected solution.

3a.4.5.4800. Requirements shall be specified in accordance with the design basis of the nuclear power plant for the probability of an operation failure when actuation is requested and, in the case of instrumentation and control systems included in Safety Class ABOS 2, relating to the frequency of false operation.

3a.4.5.4900. The components of instrumentation and control systems included in safety classes shall be fully tested in the given environment, with the preliminary determination of the testing and acceptance criteria.

3a.4.5.5000. It shall be ensured by appropriate design solutions and measures that the instrumentation and control systems may only be accessed, both physically and logically, only by persons required and allowed to do so and only at a level and with the options that allow the performance of the tasks assigned to them.

3a.4.5.5300. During the design of programmable instrumentation and control the relevant parts of the of the Design Basis Threat and the provisions of the Govt. Decree on the physical protection of use of atomic energy shall also be taken into account.

3a.4.5.5400. The protection considerations of programmable systems shall also be taken into account in the design. If, during design, the protection considerations of nuclear safety and the programmable systems are in conflict, the consideration of nuclear safety shall take priority.

3a.4.5.5500. In the Preliminary Safety Analysis Report and the Final Safety Analysis Report, in connection with the instrumentation and control of the nuclear power plant unit, the physical possibilities of modification in functions, programs and data, as well as of access posing a risk to information technology and instrumentation safety shall be defined, with a distinction of rigid wiring, including the logic manufactured with semiconductor-based circuits, and programmed instruments. These options shall be ranked by feasibility and the level of expertise necessary to achieve the modification.

3a.4.5.5600. The irregularities of programmable equipment shall be detected. It shall be ensured that the program and the constant date filed can be checked according to reliable data generated during installation and read from non-rewritable data carriers. Where it is reasonably achievable, the credibility of the data read from the technology shall be examined.

3a.4.5.5700. The systems and equipment that operate executive devices belonging to protection and safety systems and that provide functions collecting and displaying data important to nuclear safety, which influence the decisions of operating personnel, shall be protected against external influences, which allow the alteration of a safety function.

3a.4.5.5800. The possibilities of physical access and the placement of the data transmission equipment and data cables shall be designed in accordance with the physical protection zones.

3a.4.5.5900.The necessary administrative system and the safety protocol of the associated internal procedure and access shall be developed for:

a) the performance of maintenance necessary in the systems,

b) the necessary modification of the digital systems,

c) the detected program and data errors, and

d) monitoring of the inward and outward transport of data carriers.

3a.4.5.6000. Configuration management of instrumentation and control shall also cover the following areas:

a) documentation of the system and components, also in the case of commercial products,

b) hardware documentation,

c) all forms of software documentation and codes, among others, specifications, design documents, source codes, executable codes, computer codes and directories,

d) development systems, including core generators, translator programs, test environments and test tools,

e) test cases and results,

f) modifications and related analyses, and

g) *training materials.*

The Nuclear Safeguards requirements governed by the IRMr:

Section 5. (1) The organization possessing nuclear material shall maintain a local accountancy system for nuclear materials falling under its provision. The local accountancy system shall meet the requirements described in the Safeguards Agreement.

(5) The local accountancy system shall be maintained in such a way that the categories and quantities of nuclear materials possessed by the organization and their content of fissionable material can be determined any time by elements (uranium, plutonium, thorium).

Section 6. (6) The organization maintaining accountancy systems shall ensure the security of accountancy and operating records, and prevent the unauthorized access to these data.

1.3. International and domestic recommendations

The primary purpose of the elaboration of IAEA Nuclear Security Series 17 – Computer Security at Nuclear Facilities was to draw attention to the importance of computer security as part of the overall planning of the nuclear facilities' physical protection. The publication outlines the methods, frameworks and implementation procedures for implementing the computer security plan.

Standards compatible with the IEC 61513 *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems* principal standard in the field of protection of programmable systems and components are as follows:

a) IEC 61226 Edition 3.0 (2009) Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

b) IEC 60987 ed2.0 (2007) Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems

c) IEC 60880:2006 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category "A" functions

d) IEC 62138 (2004) Nuclear power plants –Instrumentation and control important for safety –Software aspects for computer-based systems performing category "B" or "C" functions

e) IEC 62645 Ed.1: Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems

Compliance with the standards on the safety categorization of I&C functions and on the implementation of hardware and software components of Category "A", "B" and "C" function is first of all important from nuclear safety aspects; however, following these standards and the so realized system and component features can be major contributors to the realization of the protection objectives.

The errors and operation anomalies may mean security gaps in software products. Elimination of errors is the first level of protection, one of the solutions is when the software development is performed in line with quality management systems. Part 3 of standard series ISO 9000 on quality management and quality assurance issued in 1997 supported this activity *"Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software"*.

The standards were re-published in 2004 with the contribution of the IEC standardization body under the identifier ISO/IEC 90003:2004. The standard provides guidance to application of quality assurance principles realized in the standard ISO 9001:2000 for procurement, development, operation and maintenance of software products and supporting services. The Guideline serves with guidance on:

a) aspects to be included in trading contracts,

b) products available on the market,

c) support of internal procedures of organizations,

d) aspects of software products embedded in hardware products, and

e) services related to software products.

According to the preamble of the software standard the document, however, does not represent a criterion for the audit of the quality assurance systems.

The standard ISO/IEC 9000-3:2004 provides guidance irrespective of all process equipment on the life cycle models, development process, and sequence of the particular activities and on the task-oriented organizational structure of the company, engineering bureau or other organization. Further standards and technical reports are available about additional aspects of software development, operation and maintenance in the software engineering standard ISO 9001:2000: ISO/IEC 12207, ISO/IEC TR 9126, ISO/IEC 14598, ISO/IEC 15939 and ISO/IEC TR 15504.

Nowadays, the basic standard of computer security is the standard ISO/IEC 27000:2012, which overviews the information security management systems, and defines related terms and definitions.

Another member of the standard series, the standard ISO/IEC 27001:2005 undertakes to cover all types of organizations including companies in the market, governmental bodies or non-profit organizations. The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's overall business risks. It specifies requirements for the implementation of protection controls customized to the needs of individual organizations or parts thereof. The application of the standard requirements ensures the selection of adequate and proportionate protection controls that protect information assets and give confidence to interested parties without hindering the cooperation with other organizations but complying with the laws. The standard is suitable for internal and external auditors.

The next member of the series is the ISO/IEC 27002:2005 standard that comprises several former standards. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management, by generally formulating objectives and describing the best practices in the field of:

a) security policy;

b) organization of information security;

c) maintenance of real estates, devices and other technical equipment owned by the organization (asset management);

d) control of access to the these;

e) human risks;

f) physical protection and security including environmental factors;

g) communications and operations management;

h) information systems acquisition, development and maintenance;

i) information security incident management;

j) business sustainability management;

k) compliance with the requirements.

The objectives and instruments of the management should be based on risk assessment and the internal security standards of the organization should specify the tasks such a way that they can support the effective security management, while not hindering the external relations operated on the basis of confidence.

The standard ISO/IEC 27010:2012 provides guidelines for implementing information security management within information sharing communities. The standard should be applied due to the nature of the problems by companies, engineering bureaus and service providers cooperating within the nuclear industry to exchange and sharing of sensitive information, including the regulatory organizations. The standard is relevant in the design, commissioning and later operation of technical developments, nuclear facilities and their process systems. The standard also can be used for the protection of the critical infrastructure.

The committee of IEC 45 recommends the following in the preamble of the standards IEC62645 (draft) for the nuclear facilities in order to avoid threats to computer systems

a) Such standards, like the ISO/IEC 27000, 27001 and 27002 should not be applied directly for programmable systems and components of nuclear facilities because of their specific characteristics.

b) Use of general industry standards and other guidelines on avoidance of threats to computers may yield benefits, but it is not sufficient for nuclear facilities.

c) Each regulation should harmonize with the principal standard IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.*

The threats to computer systems might impair the operation of the nuclear facility and its nuclear safety, and might lead to endangering the operating organization, the environment or the population living there. The target of computer system threats is the equipment and the process and not the digital system itself. The digital systems can be the instruments of an attack.

The failure and unavailability of I&C may degrade the safety of the nuclear facility to an unacceptable level and thereby may increase the risk of a nuclear accident, a reactor fuel damage, a core melt and a large radioactive release. Threats to computers in a nuclear facility might lead to much larger damages than in other industries.

Threats to computers may entail risks to critical equipment, such as the turbine or unit transformers, the damage to which can cause costly repairs and long term outages in energy production.

A nuclear facility is such a safety critical application, which requires fast, real time responses in an aggravating situation. The operating organization should also react quickly to such incidents and should make use of process parameters for doing that and should be able to rely on the truthfulness of the data.

The use of standards ISO/IEC 27000, 27001 and 27002 is very important for the companies, organizations providing engineering and computer services involved in the design, fabrication and qualification and, after installation in the facility, in the operation and maintenance of process systems of nuclear facilities. The protection of I&C associated with the process, however, required the application of additional requirements that should be considered together with the regulations on nuclear safety and physical protection.

In Hungary, the Inter-ministerial Committee for Informatics published recommendations. Protection requirements for IT systems are determined in Recommendation 12, which was published by the Informatics Coordination Office of the Prime Minister's Office in 1996. According to that computer protection can be defined as the state when the protection of the computer system, from the aspect of confidentiality, authenticity, integrity and availability of the data managed by the system, is *closed, full, continuous and proportional to the risks*.

The currently available recommendations of the Inter-ministerial Committee for Informatics (http://www.itb.hu/ajanlasok/) address the following topics:

a) Guidelines for development and implementation of informatics strategy;

b) Informatics strategic design in practice;

c) SSADM structured system analysis and design methodology;

d) Introduction to PRINCE project management methodology;

e) Guidelines of open system products complying with X/Open specification;

f) Procurement recommendations;

g) Specifications of X/Open XPG4 (XPG3) based on GOSIP4 government OSI profile;

h) Informatics security methodology manual;

i) Quality management;

j) Protection requirements for informatics systems;

k) Internet in the government - intranet;

l) Infrastructure management;

m) Common Criteria (CC), methodology of security analysis of informatics products and systems;

n) Electronic data exchange.

An important provision is contained in Commission Recommendation 2009/120/EURATOM of 11 February 2009 on the implementation of nuclear material accountancy and control system by operators of nuclear installations. Section 6 states that *a data-processing system should be implemented producing safe and secure storage of all data required for the proper working of the NMAC system,* data processing system should provide the information required by Regulation (EURATOM) No. 302/2005 and also maintain traceability for all the information provided. It should be possible to identify any information or data that could be needed to resolve discrepancies and anomalies arising from the requirements of Regulation (EURATOM) No. 302/2005.

1.3.1. General principles

Reference is often made to risk analysis in the Guideline. Subsection (1) of Section 20 of Govt. Decree 190/2011 (IX.19) Korm. prescribes the security of programmable systems proportionally to the risks. In the Guideline these

terms mean that the appropriate analyses and applied security should be completed and constructed so that they are always proportionate to the threat of the protected programmable system. In this context, we believe the ALARA principle, already proven in radiation protection can be utilized well: The radiation exposure of persons working in radiation hazardous workplaces must be kept at a level as low as reasonably achievable, taking into consideration the economic and social factors. Consequently the analogy with the ALARA principle can be formulated as follows: analyses and protection must be carried out and implemented at the highest level reasonably achievable, taking into account the economic and social factors.

The basic principle of the protection of physical systems is the principle of graded approach. This means that the applied security measures must at all times be proportionate to the likely consequences of the attack.

2. DEFINITIONS AND ABBREVIATIONS

2.1. Definitions

The Guideline contains the following definitions in addition to those in Section 2 of the Act on Atomic Energy and Section 2 of the Govt. Decree 190/2011 (IX.19) Korm.

Data:

Data is the carrier of information, a formalized representation of facts, concepts or instructions, suitable for communication, display or handling by humans or automatic devices.

Confidentiality:

A property of a piece of data which tells that only the authorized entities can access, use and decide on the use of the data and only according to their authorization.

Intrusion testing:

A test method used in the vulnerability assessment, in which the investigator with specific constraints attempts to bypass or circumvent the system security controls to gain access to the system.

Accountability:

A guarantee that the executor of data operations can be identified later.

User:

A person trained and authorized to use the informatics system and who uses protected information according to his/her work description or contract. The term “user” stands also for the representative of authority with inspection rights, as appropriate.

Access control system

Such instruments and modes that ensure that a duly authorized person can access the given system in line with the protection requirements.

Perimeter:

The logical border that surrounds a set of critical instruments connected to a network to which access is controlled.

Alternative protection control:

The use of a security control in addition to or in conjunction with a security control that has at least the same strength as the original control.

Authenticity:

A property of data which tells if it comes from the expected source.

Authentication:

Checking the identity of a user, process or device. It is often a prerequisite for access to resources.

Information:

Information about observation, experience or knowledge in readily accessible form about certain facts, or phenomena which changes, transforms, substantially affects, reduces or eliminates the uncertainty of someone's knowledge.

Information Security:

The preservation of confidentiality, integrity and availability of information.

Comment: Other properties of information might also be considered here, like authenticity, accountability and non-repudiation (and reliability).

High-energy radio frequency or microwave electromagnetic radiation source:

10% of the public health limit for electrical, magnetic and electromagnetic fields at 0 Hz to 300 GHz frequencies, and high-energy radio frequency or microwave electromagnetic radiation source in the vicinity of the protected facility is considered to be present if detectable and measurable effects are observed on the conductor, semiconductor and components containing polar molecules of the device set to be protected.

Cyber-attack:

An operation or event that could compromise the security or safety of the programmable systems.

Risk:

The extent of the possibility that a particular threat exploits the vulnerabilities of a particular system, or a group of systems, causing damage to the operating organization. The measurement is the product of the probability of the attack (T), which is determined by motivation, ability and malicious intent, the probability of success of the attack (S), which depends on vulnerability, and the consequence (K). Risk = T x S x K.

Risk management:

A process that addresses the risk of the operation of programmable systems and components that affect the operation of the organization (including the mission, function, reputation etc.), the organization's assets, personnel, other organizations and the nation. It includes risk analysis, the

realization of risk reducing strategies as well as the use of tools and procedures to continuously monitor the protection status.

Risk management framework:

Provides a structured process that integrates the protection of programmable systems and components and risk management activities into the life-cycle of the programmable systems and components.

Non-repudiation:

A property of a data which serves suitable evidence on the supervision of activities implemented in the programmable system and component.

Residual risk:

Remaining risk after the implementation of protection control measures.

Minimum user number:

In certain cases, the number of staff having access to programmable systems and components is recommended to be limited to the necessary level or to an absolute minimum level. The minimum level of limitation should be reasoned.

Very fast electromagnetic impulse:

Electromagnetic radiation in the 300 MHz – 300 GHz (wavelength: 1m – 1mm) microwave band or higher frequency harmonics, which are spontaneously created during natural phenomenon (e.g. lightning) or by man-made devices, including the possibility of modulation used in telecommunication technology for information transmission. Such impulses, if of high energy, can through their physical effects, damage electronics or electrical systems or create effects that may develop into damages. Low energy impulses can temporarily affect the operation of the electronic and electrical systems and devices without direct degradation and damage, since impulses may represent a similar effect to data transmission.

Log:

A text file that is being taken during the continuous operation of the programmable systems and components on operation and status of the system and the circumstances of potential failures, errors or other events.

Programmable systems and components:

Devices capable of performing computing, IT, communication or controlling tasks, including but not limited to e.g. personal computers (desktop or portable), mainframes, servers, network devices etc, but also lower level

devices, such as embedded systems, programmable logic controllers etc, that is, any device exposed to any kind of electronic threat.

Protection of programmable systems and components:

Comment: the term safety is used in this Guideline exclusively to refer to nuclear safety, the term security is used exclusively to refer to nuclear security, while in case of issues related to safety, security and peaceful use together, always protection is used.

Programmable systems and components protection officer:

The head of the organizational unit established or designated in accordance with Subsection (3) of Section 20 of Govt. Decree 190/2011 (IX.19.) Korm. directly under the supervision of the senior management, responsible for the protection of the programmable systems.

Protection policy of the programmable systems and components:

Such set of computer system protection principles effective for one particular organization, which affects the operation of the whole organization. This document specifies the demanded relation of the organization and members of the organization with the security of programmable systems and components and the principles of enforcement for the whole institution. The protection policy of the programmable systems and components should serve as a basis for the uniformly structured protection plan of programmable systems and components that is effective for the whole institution and is in harmony with the regulations of other fields.

Programmable system protection organizational unit:

The organizational unit established or designated in accordance with Subsection (3) of Section 20 of Govt. Decree 190/2011 (IX.19.) Korm. directly under the supervision of the senior management, responsible for the protection of the programmable systems

Availability

A property of a data or a programmable system or component of being accessible and usable upon demand by an authorized entity at and for the necessary time.

Vulnerability:

An error or a weak point in the design, implementation or operation and management of the programmable system which can be exploited by the various sources of threats.

Vulnerability assessment:

Test for detecting system vulnerabilities.

Integrity:

A property of a data which tells if the content and properties of the data are in line with the expected content and properties including authenticity, non-repudiation.

A property of a programmable system or component which tells if the system or component can be used as intended.

Social engineering:

Social engineering (psychological manipulation) uses persuasion, deception, to persuade or manipulate people into thinking that the social engineer really is who they claim to be. As a result, the social engineer – with or without the use of technology – is able to take advantage of people in order to gain information.

Attack vector:

A route, mode or device that the attacker uses to attack the target.

Attack tree:

A tree structure conceptual diagram showing the ways to the target that is defined as the root node.

Attack graph:

The attack graph is a representation of a target and its associated attack possibilities, tools and modes that can model the attack against the target by revealing the interdependencies (relationships) between the various elements (nodes).

Remote access:

Remote access is when any user accesses or uses data, programs, informatics instruments via the signal transmission system of a programmable system or component across the protection levels.

Remote maintenance:

That remote access can be considered as a remote maintenance action, the purpose of which is the maintenance of the status, original operability and reliability of systems and devices. Its form can be information collection, processing and management related to processes and devices. Remote

software updates and installation of software elements with the aim of development are also considered as remote maintenance.

Protection event:

Any perceptible or distinct event that is relevant to the operation of the programmable systems and components or the provision of a service, and the assessment of the effect that a particular deviation may cause in the services.

Protection incident:

Intentionally or accidentally occurring protection event (or a series of events) that effectively or potentially endangers the confidentiality, integrity or availability of the programmable system or information stored, processed or transmitted therein, or violates the protection policy, procedures or related policies or is in direct danger of it.

Protection control:

Protection controls are all those technical (logical), physical and administrative protection measures whose application ensures the protection of programmable systems and components against unintended damages caused by humans and against cyber-attacks defined in the design threat basis.

Protection requirement:

A set of policies, regulations, rules and procedures that prescribe how an organization manages and protects its programmable systems and components.

Protection programme:

The protection programme manages and prioritizes the processes and activities that address the protection of programmable systems and components from different point perspectives in order to achieve the protection goals.

Protection level:

The protection achieved through the implementation of protection control measures established by the risk analysis by identifying residual risk. The protection level is acceptable if the level of residual risk is acceptable.

Protection zone:

The protection zone groups the programmable systems and components together according to the identified risks. Programmable systems and components belonging to the same protection zone correspond to the

same human, physical or cybersecurity requirements, thus have the same protection level.

2.2. Abbreviations

CPU	Central Processing Unit
DMZ	De-Militarized Zone
FAT	Factory Acceptance Test
FPGA	Field Programmable Gate Array
HIDS	Host Intrusion Detection System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
NSC	Nuclear Safety Code, i.e. Annex 1 through 10 of Govt. Decree 118/2011 (VII.11) to which reference is made as the Volumes of the NSC
PLC	Programmable Logic Controller
PKI	Public Key Infrastructure
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAT	Site Acceptance Test
USB	Universal Serial Bus
UTM	Unified Threat Management
VPN	Virtual Private Network
WLAN	Wireless Lan

3. RECOMMENDATIONS OF THE GUIDELINE

3.1. Organization of protection of programmable systems and components, responsibilities

3.1.1. Responsibilities of the licensing organization and the senior management of the facility

The licensing organization and the senior management of the facility must be aware of the fact that programmable systems and components are becoming widely used in the facility to perform vital activities related to nuclear safety, physical protection, safeguards, and radiation protection. This development has several benefits in terms of nuclear safety, physical protection, safeguards and radiation protection. In order to best utilize these benefits the safe operation of programmable systems and components must be ensure through adequate and balanced protection measures. The protection measures must maximize protection against external influences, unintentional and intentional (malicious) acts without unnecessarily hindering the operation of the systems.

The senior management of the licensed facility should assume overall responsibility for the introduction and compliance of protection requirements for the programmable systems and components with the legislative background. In order for that:

a) It should define the protection objective for programmable systems and components of the facility,

b) It should determine the level of acceptable risks for programmable systems and components,

c) It should ensure that the facility has an effective protection policy for programmable systems and components,

d) it should provide sufficient resources for the performance of the tasks related to the protection of programmable systems and components,

e) it should ensure repeated and periodic audits and updates of the protection policy and protection procedures for programmable systems and components,

f) it should ensure support for initial and refreshing trainings and awareness programmes corresponding to the protection of programmable systems and components.

The protection policy for programmable systems policy must be a part of the physical protection policy of the nuclear facility (the protection policy is either a stand-alone document or a part of the facility's quality assurance

policy). The protection policy defines the general, high level security objectives in relations to the programmable systems of the facility, in line with the objectives of nuclear safety, physical protection, safeguards, and radiation protection, taking into account its legal and human resources impact.

The requirements set out in the protection policy of the programmable systems and components must be broken down into lower level documents that may be used during the implementation and control. The objectives formulated in the protection policy of the programmable systems and components must be enforceable, executeable and verifiable.

The senior management of the licensing organization's facility must establish or designate an organizational body for carrying out monitoring and coordination activities related to the protection of the programmable systems. The head of this organizational unit is the programmable systems and components protection officer, who is under direct supervision of the senior management. In addition to the programmable systems and components protection officer the organizational unit consists of his/her direct subordinates and/or the protection team designated by the persons responsible for the operation of the programmable systems and the operation of the protection measures of the programmable systems.

3.1.2. Programmable systems and components protection officer

Programmable systems and components protection officer is a manager directly subordinated to the senior management of the facility, who

a) leads the organization tasked with the protection of programmable systems and components,

b) controls and coordinates the adequacy of protection tasks of the programmable systems and components,

c) controls and coordinates the definition of the design basis of the protection tasks of the programmable systems and components in the facility and the adequacy of the solutions based on them,

d) cooperates with the organizations responsible for nuclear safety, physical protection, implementation of safeguards requirements and radiation protection in order to coordinate protection tasks,

e) ensure information exchange among the organizations performing protection tasks of programmable systems and components,

f) arranges the periodic risk analysis of the programmable systems and components of the facility through the and determines the critical elements of the facility based on its results.

g) initiates periodic inspections, audits and reviews of the protection measures of the programmable systems and components and the adequacy of the resources allocated to them, and provides a status report of the inspections and their results as well as recommendations to senior management,

h) arranges for the establishment of the protection training procedures associated with programmable systems and components, follows and monitors the implementation, adequacy and continuous development of the training courses,

i) checks and reviews the adequacy of the protection tasks and on the basis of this propose procedures, measures for abnormal situations, and cooperate with the relevant internal and external organizations,

j) Coordinates the investigation of protection incident related to programmable systems and components, and monitors the implementation of measures taken on the basis of the investigation report.

3.1.3. Programmable systems and components protection team

Within their working area, the member of the programmable systems and components protection team should be responsible for:

a) Adequate implementation of the objectives determined in the protection policy for programmable systems and components of the facility,

b) Adequate information of the programmable systems and components protection officer if any change in relation to the security of programmable systems and components takes place,

c) Design, development and implementation of protection improvement measures for programmable systems and components and in cooperation with the organizations concerned, supervision of their implementation.

3.1.4. Responsibilities of the heads of organizational units

The head of each organizational unit of the facility is responsible for ensuring the uninterrupted cooperation between the protection officer of the programmable systems and components and the supervision of protection, as well as, the development and implementation of the protection measures for the organizational unit.

The head of the organizational units that provide or perform protective activities are responsible for delegating a representative to the protection team, ensuring that the representative is allocate the required work-time

for training and cooperation purposes with the supervisory activities contained in the protection tasks.

3.1.5. Responsibilities and obligations of all employees of the facility

Each employee of the facility is responsible for:

a) Knowledge of the baseline protection procedures of the programmable systems and components;

b) Knowledge of job specific protection procedures of programmable systems and components;

c) Working according to the objectives set in the protection policy for programmable systems and component of the facility.

Each employee of the facility is obliged to:

a) Notify his/her supervisor of any conditions, actual or probable event that may lead to change, decrease or degradation in the protection level of programmable systems and components.

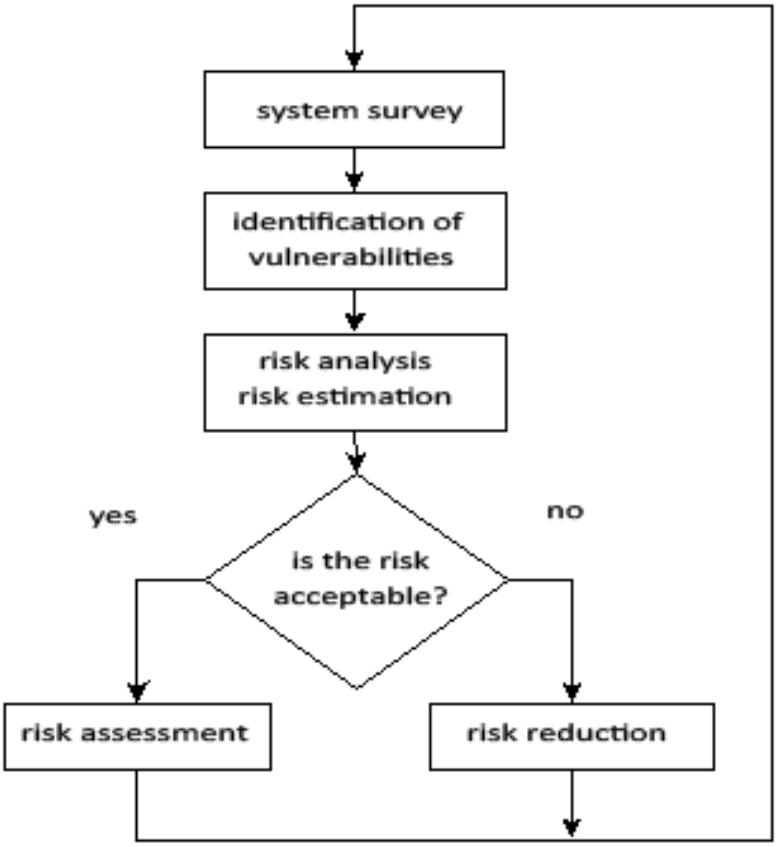
b) Participate in the basic and further protection trainings related to programmable systems and components.

3.2. Protection classification of programmable systems and components

The protection classification of programmable systems and components shall be based on their nuclear safety, physical protection, safeguards and radioactive material inventory functions, based on the risk analysis of the particular programmable system.

The protection of programmable systems and components means reducing the risks to below acceptable levels. Thus, risk analysis is the fundamental starting point for designing the defense in depth zones and for designing the protection measures, while also serving as a proof of the adequacy of the established protection levels.

3.2.1. Risk analysis (threat analysis, vulnerability analysis, risk assessment)



3.2.1.1. Basics of risk and risk definition

The risk of programmable systems and components is the extent of the possibility that a particular threat exploits the vulnerabilities of a given system or a group of systems, causing damage to the organization operating the system. Measurement is based on a combination of the probability of occurrence of an event and the consequences of thereof:

$$r = \sum_{t \in T} (p_t \cdot d_t),$$

Where r is the risk, T is the set of relevant threats, pt is the probability (frequency) of the occurrence of a given threat, dt is the damage resulting from a given threat.

When determining the risk for the programmable systems and components of a nuclear facility, the primary risk factor to be taken into consideration is the risk

The primary risk factor to be taken into consideration when determining the risk of the programmable systems and components in a nuclear facility is the risk of nuclear safety being compromised. When determining the risk,

the risk of damage to the protection of the programmable systems and the damage to the physical protection of the programmable systems must also be taken into account.

Design Basis Threat (DBT) must also be taken into consideration for the risk analysis of the programmable systems. Knowledge of the DBT is needed to properly assess the risks, the determination of which is expedient to be made, so that is available in a timely manner.

In addition, further risks can also be taken into account (e.g. operation objectives, risks arising from damage to business interest). These are identified by the organization responsible for the protection of the programmable systems and components of the given facility, in cooperation and in agreement with the other organizational units of the facility.

The characteristics, assumptions, requirements and the methods of analysis used to determine the risks should be documented. The protection level of each programmable systems and components is determined by the organization responsible for the protection of the programmable systems based on the results of the risk analysis and with due regard to the guidance provided in 3.2.2.

Risk analysis should also be carried out for pre-commissioned or already operating programmable systems, for the following reasons:

a) (for new facilities) To demonstrate the planned protection capability of the established system.

b) (for operating facilities) To confirm the preservation of the protection capabilities after a modification.

c) The risks and their probabilities have changed.

3.2.1.2. Risk assessment and management

Risk assessment facilitates the decisions to determine which resources are to be used to manage which vulnerability as well to reduce the likelihood of probability of their exploitation.

The risk evaluation is a process, during which certain threats, vulnerabilities and effects are identified, and then appropriate protection mechanisms are associated with them. The countermeasures addressing the prevention of attacks against programmable systems and components as well as the mitigation of their potential consequences should be based on the assessment of threats and vulnerabilities.

The basic steps of risk analysis and risk management are the following:

a) Determination of perimeters and perimeter effects

b) identification and characterization of threats,

c) assessment of vulnerabilities,

d) development of attack scenarios,

e) determining the probability of a successful exploitation of a given vulnerability,

f) determination of risk level,

g) development of countermeasures.

Appropriate and well defined process should be applied for the systematic and consistent conduct of risk assessment and evaluation tasks. Several effective risk assessment and management methodologies and tools are currently available; most of them are based on well-known terms and logics. The risk assessment and management methodology should be the methodology described in the ISO/IEC 27005 international standard; however other internationally recognized methodologies may also be applied.

The necessity of the conduct of a risk assessment in relation to certain systems, the depth of the assessment and the frequency of updating the assessment are dependent on the importance of the safety and physical protection functions of the system. A new assessment should be conducted or at least its former version should be revised, if a modification is implemented on the system. Such modifications may be induced by new equipment, software, procedures, or a significant change in the operatory expertise. The threat to and vulnerabilities of connected systems are usually greater than those operating in island mode.

If the risk assessment cannot be conducted concerning certain threats, then the best practices and the good engineering solutions should be applied.

The basic steps of risk analysis and risk management the following:

a) Determination of perimeters and perimeter effect,

   – The purpose, scope and the conditions under which the analysis is to be carried out must be determined. The scope should be determined on the basis of the list of programmable systems and components, which shall include all the information and data necessary to carry out the risk analysis.

b) Identification and characterization of threats, assessment of vulnerabilities,

- Information on the sources of threats, the vulnerabilities and their impacts must be collected, including information of the DBT that will be used during the analysis. The risk model and evaluation or assessment approach to be used should be determined or specified.
- Based on the DBT, account should be taken of who can pose a threat, where they may be located (within or outside the country, inside the facility), what capabilities they may have, what their intentions and motives are and what they can access.
- The sources of threats should be determined based on their types (intentional, accidental, structural, environmental). Among these, the ones that threaten the assessed system should be chosen. In the case of intentional threats, the ability, intent and aim should be assessed. In the case of unintended threats the range of the impact, the spread.
- The vulnerabilities and sources should be determined together, as well as the circumstances which can increase the vulnerabilities or cause new ones. The severity of the vulnerabilities needs must be evaluated.
- The expected residual risk should be determined based on the protection zone model.

c) Development of attack scenarios,
   - Attack vectors, attack profiles and attack scenarios should be developed and the estimation of the resource needs should be performed.

d) determining the probability of a successful exploitation of a given vulnerability,
   - It is necessary to estimate the probability of the occurrence of an attack event and the probability of its success in terms of the damage. The range of the estimated probabilities depends on the analytical model used. They may take on qualitative values (e.g. very high, high, medium, low or very low) or quasi quantitative values (e.g. 10, 8, 5, 2, 0).

e) Determination of the risk level,
   - The damages caused by the attack events and their consequences should be analyzed and the magnitude of the consequences should be defined for which qualitative or quasi quantitative mapping can also be used. For programmable systems and components, the primary consideration should be given to consequences related to nuclear safety. The consequences of the attack events should be

analyzed with regard to the planned operating conditions of the facility and for the transitions between the planned operating conditions.

- Risks should be determined on the basis of their probability and consequences and the risks should be prioritized.
- The results of the risk assessment must be communicated to those affected and the method of communication (report, dashboard, etc.) should be determined. The results and the supporting evidence must be shared in accordance with the rules and regulations.

f) Development of countermeasures.

Risk management procedures must be developed for the risks identified as a result of the risk analysis in order to reduce the risks and for the residual risks to be acceptable. Risk management options:

a) Risk reduction through defining protective measures. After implementing the specified protection measures the level of residual risk must be measured to see whether it has fallen below the desired level.

b) Risk retention. Conscious decision, does not require action.

c) Risk avoidance. Avoiding risks by changing the conditions or activities e.g. disabling the vulnerable feature or function.

d) Risk transfer to others who can handle it. For example insurance coverage.

The above recommendations for risk analysis and risk management should also be followed in the case of an operating nuclear facility, subject to the acknowledgement and analysis of the circumstance that the protection zone model has to adapt to the features of an existing facility, having regard to its existing architectural, technological, I&C and physical protection properties.

3.2.1.3. Identification and characterization of threats.

The first step of planning the protection of programmable systems is the identification of the potential threats based on the systematic characterization of potential adversaries and attack scenarios. The overall characterization of the adversary capabilities compiles from the identification of the potential adversary types, their motivations and the potential targets. Subsequently, attack scenarios should be developed based on the overall characterization. The assessment of the threat against

programmable systems might be supported by the National Network Protection Centre (PTA CERT-Hungary) and the National Security Office.

The characters, pre-assumptions, requirements and assessment methods to be applied during the risk assessment should be selected by the organization responsible for the protection of the programmable systems and components in cooperation and agreement with other organizations of the facility. The selected characteristics, pre-assumptions and requirements and assessment methods should be documented, including the considered risk factors, vulnerabilities, threats, adversary capabilities and potential, the likelihoods and consequences, as well as all those additional factors that were taken into consideration during the planning of the management system and architecture of the protection of programmable systems and components. All of the above is defined as the design basis threat.

3.2.1.4. Vulnerability assessment

The purpose of the vulnerability assessment is to detect possible vulnerabilities of the programmable systems and components.

During the life cycle of the programmable systems and components, the vulnerability assessment should be performed as follows:

a) In the design phase, the programmable systems and components should be designed so to minimize their vulnerabilities even without the use of protection controls (secure by design). The vulnerabilities should be paid attention to also when purchasing completed programmable systems and components, therefore the protection officer should also be involved in the procurement decisions. A list of known vulnerabilities should be obtained from open databases or from the vendor.

b) During manufacturing, the manufacturer must ensure that the manufacturing process does not produce any vulnerabilities. The manufacturer must prevent unauthorized access to the programmable systems and components, must provide the latest updates and must conduct the vulnerability assessment by having all the information in their possession and transfer the assessment report with the programmable systems and components. The assessment report must be used for the risk analysis to be carried out for the application of a construction license, and must be attached to the application for the construction license.

c) The vendor must provide the installed programmable systems and components with the latest updates in accordance with the provisions contained in the Patch Management guideline, must change the default security settings (e.g. user name, password) and must conduct the vulnerability assessment. The assessment report must be used for the

risk assessment to be carried out for the operating license and must be attached to the application for the operating license. In such cases, the programmable systems and components must be examined in their environment. Prior to testing, security updates must be installed on the programmable systems and components.

d) After installation, only systems with non-operational connections should be subject to vulnerability assessment. The tests and the test methods to be used must be approved by the HAEA and the reports must be sent to the HAEA.

e) At decommissioning the vulnerability assessment should be carried out in connection with the installation of the new programmable systems and components replacing the decommissioned system.

When preparing the vulnerability tests, the scope, direction and revealed information should be determined. The scope shall be determined on the basis of a list of the programmable systems and components. The direction of the investigation is the attack vector, which can be e.g. internet, internal wired network, that is the same or another protection zone and wireless network. Nowadays it is rare that there is no information available about the systems (black box) therefore it should be assumed that the attacker also possesses some (grey box) or all the information (white box).

Following the preparation, the following steps must be performed for the vulnerability assessment:

a) Collecting general information.

a) Collecting technical information (e.g. supplier, manufacturer, network diagram).

b) Mapping accessible systems and services using automatic tools (using IP and port scanning tools e.g. NMAP) or manually.

c) On the basis of these results, vulnerabilities should be identified by automatic vulnerability assessing tools (e.g. Nessus), which use information available in public databases. Manual testing can confirm the results of the automatic testing and can investigate special vulnerabilities (related to access, network connection and databases).

d) Determining the need to conduct penetration test and if necessary intrusion test.

e) The tests should include reviewing the documentation and source codes, reviewing the devices' configuration settings, physical testing of the devices and interviewing the staff.

The results of the assessment should be compiled in a report, which contains the detected vulnerabilities in order of importance and the proposed remedial measures. The report may contain details about the testing methods, vulnerabilities, attacks, vulnerability footprint, exploitation patters and their evidence, the effects of the vulnerability, attack scenarios, corrective measures and the conclusions by deducting lessons learned.

An important part of the report is the measurement of the detected vulnerabilities. A measurement system must be developed and accepted. It is recommended to use a widespread measurement system e.g. the Common Vulnerability Scoring System – CVSS. Measurement systems quantify the risks and effects resulting from the vulnerabilities.

3.2.2. Protection classification of programmable systems and components

Classification of programmable systems and components should be carried out according to the function fulfilled in line with the IAEA recommendations in the document *Computer Security at Nuclear Facilities.*

if the physical design of the nuclear facility does not make it possible to assign the physical protection classification and the nuclear safety classification of the systems, and systems or components having different safety classification are or may be operated at the same physical location, then protection levels can be determined only in a functional sense, however in consequence of that more rigorous rules should apply for the lower protection level digital systems of the process. The nuclear safety classification in case of a nuclear power plant is ABOS, in case of the spent fuel storage facility it is the BIOS rating system.

In the case of the commissioning of new nuclear facilities, additional recommendations are as follows:

The protection architecture of the programmable systems and components must have a system of protection zones. The organization of the protection zones must comply with the defense in depth principle. The protection zone groups programmable devices together that must meet the same protection requirements. Every device in the protection zone has a certain level of protection capability. If this protection capability is lower than required by the protection zone, additional protection controls must be utilized. Communication between the protection zones can only take place through specific and properly protected communication channels, which may be network or non-network (e.g. portable devices) communication channels.

When designing the protection zones, the similarity and importance of the function performed by the programmable devices must be taken into account, because the more critical a function is, the better protection it needs, and similar functions should be protected in similar ways. All programmable systems and components should be placed in a protection zone that can ensure the protection of the performed function according to the importance of the function. Programmable systems and components that cannot be placed this way should be treated as exceptions.

Risk analysis of the programmable systems and components should be performed. The risk analysis should define the protection capabilities, threats, vulnerabilities and the consequence of damages of the programmable systems and components. The severity of the consequences must be taken into account in order of the importance of the functions performed by the programmable systems and components. In order to measure the importance of the functions, a qualitative or quantitative measurement system should be developed and the functions should be classed so that their importance can be measured and ranked:

a) The importance of the nuclear safety functions can be deduced from the safety classes.

b) The importance of availability can be obtained from the availability requirement of the function.

c) The importance of the confidentiality of data and information shall be determined on the basis of the risk of breach of the security principle.

d) To determine the importance of the nuclear safeguards functions, risk analysis should be performed and the importance should be quantified based on the impacts and consequences.

When designing the protection zones, the physical protection zones must be taken into consideration (and vice versa) because the physical protection zones fulfil protection requirements. Every programmable system and component should preferably be placed in a protection zone that can provide the expected protection resulting from the physical protection zone. Programmable systems and components that cannot be installed this way should be treated as exceptions. The protection zone boundaries cannot cross the physical protection zone boundaries, only the communication channels can. The physical protection zone is in itself a protection control for communication channels. There may be several protection zones within a physical protection zone if justified by groups of similar protection measures. However, a minimum number of zones must be provided to ensure the necessary protection measures.

When designing the protection zones, the similarity and importance of the function performed by the programmable devices must be taken into account, because the more critical a function is, the better protection it needs. All programmable systems and components should be placed in a protection zone that can ensure the necessary protection based on the nuclear safety classification of the programmable systems and components. Programmable systems and components that cannot be installed this way should be treated as exceptions. Through the importance of the functions, the nuclear safety classifications are also a factor in the design of the protection zones.

When designing the protection zones, it is recommended to first define and then segment a larger protection zone. Effort should be made for each of the protection zones one the one hand to include as many programmable systems and components as possible, on the other that these programmable systems and components are similar to each other with regard to their required protection controls. The design of the protection zones and the classification of the programmable systems and components should be an iterative process.

The protection zones must be documented in the protection plan by providing at least the following information:

a) a description of the protection zone (name, definition, functions),

b) the boundaries of the protection zone,

c) the programmable systems and components of the protection zone,

d) result of the risk assessment of the protection zone (residual risk, the protection capabilities of the programmable systems and components, threats, vulnerabilities, consequences),

e) protection objectives (availability, integrity, confidentiality aspects briefly),

f) protection control measures,

g) external connections, including non-network channels,

h) the importance of the functions performed by the programmable systems and components in the protection zone,

i) the nuclear safety classification of the programmable systems and components in the protection zone,

j) the physical zone containing the protection zone,

k) the name of the protection zone (if any) surrounding the protection zone.

If, due to physical placement, network or functional constraints certain programmable systems and components cannot be installed in a protection zone, which could provide the necessary protection resulting from the systems' performed function and nuclear safety classification, they must be treated as exceptions and their protection must be ensured through one of the following measures:

a) Placement of the programmable systems and components in a zone that can provide greater protection than is needed. The expected residual risk is thus met, but the higher than necessary protection may have an adverse effect on the systems' functionality and use, therefore in such cases the effects of the protection measures must also be investigated.

b) Increasing the protection of the programmable systems and components through additional protection controls, which complement the surrounding protection provided by the protection zones and physical protection zone as well as the programmable systems' and components' existing protection capabilities in such a way that the residual risk is at an acceptable level.

c) Increasing the protection of the programmable systems and components by establishing a better protected protection zone around it, so that the residual risk is at an acceptable level as a result of the increased protection. It is recommended to investigate the possibility of including the neighboring programmable systems and components.

The protection zones established this way provide the required protection of the programmable systems and components assigned to them within the appropriate physical protection zones according to the importance of their functions and their nuclear safety classification. This represents the suitability of the protection zones, physical protection zones and nuclear safety classifications, which must be presented in the protection plan as follows:

a) A list of the programmable systems and components assigned to each protection zone and the supporting arguments for their assignment.

b) Description of the programmable systems and components which are treated as exceptions, a justification for the need for such exceptions and a description of adequate protection measures.

c) The optimal nature of the established protection zone with regards to the following: number of protection zones, similarity of the protection controls for the programmable systems and components in the protection zones, the number of programmable systems and components assigned to a protection zone and the number of programmable systems and components treated as exceptions.

Depending on the defined protection level, the protection capabilities of the programmable systems and components, the surrounding protection zones and the external connections, the necessary protection control measures must be developed for the protection zone and protection zone boundary (communication channels). Through the protection control measures the level of residual risk of the programmable systems and components should be reduced to acceptable levels. In order to define the protection measures of the protection zones, baseline controls must be established, which are applicable to all zones and are expanded according to the specific protection requirements of each zone. When defining the protection control requirements, the following should be taken into account:

a) The functionality of the protection controls of a single protection zone may not depend on the functionality of the protection controls of another zone (see NSC 3a.4.5.4300).

b) The protection control measures of the various protection zones surrounding each other may not contain common vulnerabilities (see NSC 3a.4.5.4700).

c) In the case of the most protected zone, reaction free nature must be ensured against lower level protection zones (see NSC 3a.4.5.3700, 3a.4.5.3800, 3a.4.5.3900). Therefore in the case of the communication channels of the most protected zone, the principle of physically one-way communication channel must be applied. The data transfer can only be from the direction of the programmable systems and components in the protection zone towards the lower level protection zones. One possible implementation of the physically guaranteed one-way data transfer principle is the use of a data diode.

d) In the most protected zone, two-way communication is only permitted between programmable systems and components within the same zone.

e) Remote access (e.g. remote maintenance, admin and monitoring via remote desktop connection or SSH sessions, FTP access) to programmable systems and devices in the most protected protection zones must be disabled.

f) Programmable systems and components in a lower level protection zones may not initiate communication with programmable systems and components at a higher protection level.

g) When transferring data, software or firmware from a lower protection level to a higher protection level, such documented validation procedures must be applied that provide a protection level at least as high as the level of protection of the target programmable system and component to which the data, software or firmware or the programmable system and component will be connected to. This way, it can be ensured that the programmable system and component is free from software, firmware, infected code, Trojan and any other passive attacks.

3.2.2.1. Programmable systems and components classified as protection level 5

Administrative and document management programmable systems and components belong to protection level 5.

Those segments of management systems should be classified to protection level 5, which are in direct connection with the physical protection system, receive data therefrom, send data thereto. A management system belongs to protection level 5 if it provides internet connection towards and physical protection subsystem or data connection towards any network that is out of the scope of this regulation.

3.2.2.2. Programmable systems and components classified as protection level 4

All expert systems belong to protection level 4. The expert systems only provide possibility to review technology data for evaluation, analysis and process planning purposes (e.g. complex calculation analysis of reactor core, determination of reactor-physics properties).

Systems of protection level 4 are operated on hardware and software devices that are physically separated from the systems of protection level 2 and 3.

Those programmable systems and components should be classified to protection level 4 which covers endpoints located at the periphery of the Physical Protection Technical System. The endpoints are the access system, video surveillance system, object or fence protection system, alert management system, control points, cameras, fence, object protection instruments and media converters of informatics signal transmission subsystem system and other equipment of the subsystems with endpoint functions. This protection level should include those workstations, which have reading, inquiry, display functions, and fulfils supplementary functions

for the access system (e.g. license plate identification, management of companions, other front office functions). The Physical Protection Technical System should by its function be able to manage the loss of endpoint system components to provide that they can be substituted with due redundancy or living force on the scene depending on the location. The protection should be constructed such a way that attacks from the direction of level 4 should be detected and arrested at level 3 and level 2.

Workstations containing the registry of nuclear and other radioactive materials should be classified as protection level 4.

3.2.2.3. Programmable systems and components classified as protection level 3

Those programmable systems and components should be classified to protection level 3, which obtain process parameter data from electrical and I&C systems directly connected to the process of the plant, from protection, interventions or control systems, or from their own independent data collectors. They are systems not directly important to nuclear safety, they do not make or they are not able to make direct intervention into the process. Programmable systems and components of protection level 3 ensure supervision of technology processes. Their functions are to support the work of operating organizations and to control of safety systems belonging to protection level 2. Accordingly, the digital systems of protection level 3 measures the parameters describing the technology process on a continuous basis as well as collect, process and display them for the operating organization. The measured or calculated parameters are stored for subsequent evaluation.

Those measurement data collectors of programmable systems belong to protection level 3, which perform cyclic inquiry, transformation, primer processing and forwarding of measurement signal from the technology towards the central computers.

Those systems and components of the Physical Protection Technical System should be classified to protection level 3 which, if influenced, may cause local loss of systems at the are controlled by the subsystem concerned. Such a system component can be the access system, video surveillance system, object or fence protection system, alert management system, sub-centres, signal transmission and control cabinets of informatics signal transmission subsystem, active devices of informatics network and those workstations through which the local parameters of various system components can be modified. The listed system components locally serve the signal processing equipment of protection level 2 system centres. Because the Physical Protection System consists of several different main systems (e.g. technical system, guard service, control system,

communication system) and its technical system consists of several subsystems, while the subsystems consist of several protection zones, the Physical Protection System, by its design, should manage local losses with appropriate effectiveness. The protection should be constructed such a way that attacks from the direction of level 3 should be detected by the protection equipment of the level 2 system centre.

In the case of the final repository of radioactive waste, systems classified by BIOS as priority can be classified as protection level 3 according to the ALARA principle, because it is unlikely that a high thermal output of MW magnitude will be generated resulting from the intentional malfunction of the programmable devices.

3.2.2.4. Programmable systems and components classified as protection level 2

All programmable systems relevant from nuclear safety aspects fulfilling electric or I&C intervention, control or protection function (e.g. reactor protection system) should be classified into protection level 2. Operation of control and protection systems is meant to protect a larger part of technology, equipment or even the whole unit against hazards from parameter exceedance and failures. Their operation may trigger shutdown of a process or the whole operation. Identification of the initiating events endangering safety of main equipment, automatic triggering of interventions associated with the given event, process parameter display used to identify the event, provision for possibility for operatory triggering of safety interventions are the tasks of such systems.

Data for further calculations can be transmitted towards security level 3 systems via one way connection, which is free from reaction.

All such systems components of the Physical Protection Technical Systems should be classified into protection level 2, the loss of which may cause significant availability problem in the operation of the technical system, such as the total loss of the access, video surveillance, object and fence protection system or the alert management, informatics signal transmission subsystem. Those databases should be classified into protection level 2, the knowledge, influence of data stored in which basically affect the availability, authenticity and confidentiality of the technical system.

System centres, server computers, intrusion detector devices (firewall), databases of the physical protection systems should be classified into this security level, because a successful attack against these components the consequences would affect the whole subsystem, and an undetected modification of the databases or data gain from them would cause serious consequences.

3.2.2.5. Programmable systems and components classified as protection level 1

Systems classified as level 1 of the nuclear safety classification should be classified as protection level 1 systems. There is no facility in Hungary where it would be necessary to operate a programmable system or component belonging to protection level 1. In the case of programmable systems and components that are critical from a nuclear safety aspect, the risk analysis can result in the system being classified into a more stringent protection level, such as protection level 1.

3.2.2.6. Protection level of signal transmission routes

Data transmission between programmable systems and components may take place via optical, copper based or, in the case of radio frequency via, air as signal transmission medium.

Radio frequency transmission should be avoided, if possible, because of informatics security considerations. In the case if the technology to be applied does not allow for meeting this condition, then the total system should be reviewed from confidentiality, availability and integrity point of view in the form of a risk assessment.

General requirements for optical, copper based signal transmission cabling of programmable systems and components are as follows:

a) Cabling serving the systems should be independent of those of other systems not covered by this regulation, and its construction should support the meeting of fault tolerance criteria.

b) Unfolding of cables is allowed only in compartments and cabinets which are equipped with protection devices according to the protection level of the system.

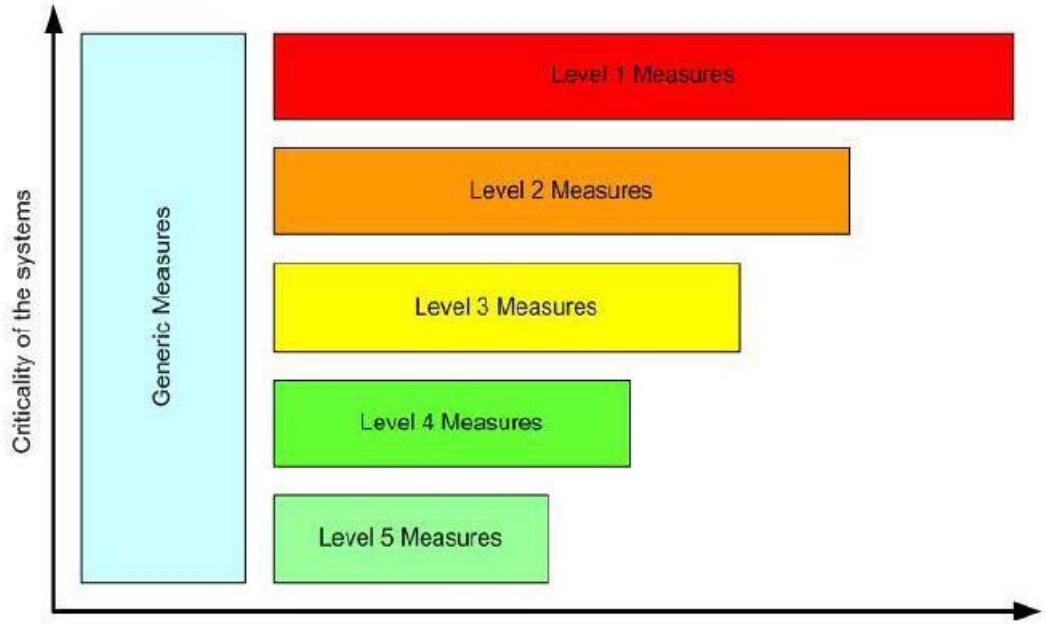
c) If the use of common trunk lines or a cable extension is unavoidable, then detection of access to the cables, cable boxes, cable ends should be solved. Risk assessment should be performed to guarantee an appropriate level of protection and to provide an effective technology solution. Use of protection solutions or a modification of cabling according to the above conclusions should be decided in line with the results of the risk assessment.

d) Electric power supply system should be constructed to comply with the availability criteria with due redundancy, protected against over-voltage, without disturbance. The adequacy of cable systems providing supply for the systems in concern should be examined in the form of risk assessment for each system and for each protection level.

Risk assessment for cabling should be performed for groups, while for critical components in details.

3.3. Requirements related to protection levels

Protection levels range from level 5 (the least rigorous protection needed) to level 1 (the most rigorous protection needed), as illustrated in the figure. The requirements corresponding to each level consist of general and level-specific requirements.



The protection architecture of the programmable systems and components is provided by the defense in depth concept (see 3.4.2.2.). Each zone has different levels of protection and the protection is stronger the deeper the protection zone is. Thus, the programmable device in a given zone is protected by the control measures for that particular zone and by the control measures in the other protection zones outside its zone.

The defense in depth is based on the risk analysis, such that the depth of the zones and the level or protection are proportional to the risk. This way the realization of the defense in depth can be verified through risk analysis. To do this, risk analysis of the programmable systems and components in the zones must be performed and the adequacy of the defense in depth can be verified by the residual risk.

The defense in depth strategy for the programmable systems and components must be designed, documented in the protection plan and implemented in accordance with the plan in order to provide the adequate level of protection. Two basic protection control measures must be in place in order to maintain protection:

a) Detecting, analyzing and avoiding deliberate or unintended damages and cyber-attacks through appropriate responses, including restoration.

b) Performing changes in a controlled manner, so that the changes do not reduce the level or protection of the system.

3.3.1. Generic requirements of protection levels

The following general measures should be applied to the systems:

a) The facility must have a document regulating policies and procedures for each level.

b) The internal policy developed under a) should apply to all users.

c) Every user must be suitably qualified and protection-informed.

d) Users should be given access to only those functions on those systems that they require to carry out their jobs, i.e. strive to minimize the number of users.

e) Ensure that appropriate access control and user authentication is in place.

f) Appropriate anomaly detection systems and procedures should be in place.

g) Application and system vulnerabilities should be monitored, and appropriate measures should be taken if necessary.

h) The vulnerabilities of the systems should be reviewed regularly.

i) Internal regulation should be developed concerning removable media and the required procedures must be carried out regularly.

j) Computer and network protection components should be strictly maintained on a periodical and continuous basis.

k) The licensee should log and monitor computer and network protection components (e.g. gateways, intrusion detection systems, intrusion prevention systems, virtual private network servers).

l) The licensee should operate appropriate data backup and recovery procedures.

m) The licensee should restrict physical access to components and systems based on their functions.

3.3.2. Special requirements of the various protection levels

3.3.2.1. Specific measures for protection level 5

In addition to the generic measures:

a) Only approved and qualified users are allowed to make modifications to the systems.

b) Access to the Internet from level 5 systems is allowed provided that adequate protective measures are applied.

c) Remote external access is allowed for authorized users provided that appropriate controls are in place.

3.3.2.2. Specific measures for protection level 4

In addition to the requirements relevant for the generic level:

a) Only approved and qualified users are allowed to make modifications to the systems.

b) Access to the Internet from level 4 systems may be given to users provided that adequate protective measures are applied.

c) Security gateways are implemented to protect this level from uncontrolled traffic from external company or site networks, and to allow specific activities which are controlled.

d) Physical connections to systems should be controlled.

e) Remote maintenance access can be allowed and controlled on a continuous basis if the compliance with protection policy defined for remote computer and user is ensured.

f) System functions available to users are controlled by access control mechanisms. Any exception to this principle should to be carefully studied and protection should be ensured by other means.

g) Remote external access can be allowed for approved users provided that appropriate access control mechanisms are in place.

3.3.2.3. Specific measures for protection level 3

In addition to the requirements relevant for the generic level:

a) Access to the Internet from level 3 systems is not allowed.

b) Licensee should continuously monitor logging and audit trails for key resources.

c) Licensee should protect this level by implementation of security gateways from uncontrolled traffic from level 4 systems, and to allow only specific and limited activity.

d) Licensee should control physical connections to systems.

e) Licensee can allow remote maintenance on a case by case basis provided that it is robustly controlled on a continuous basis; and the remote computer and user respects a defined security policy.

f) System functions available to users are controlled by access control mechanisms. Any exception to this principle should be carefully studied and protection should be ensured by other means (e.g. physical access).

3.3.2.4. Specific measures for protection level 2

In addition to the measures relevant for the generic level:

a) Only an outward, one way networked flow of data is allowed from level 2 to level 3 systems. Only necessary acknowledgment messages or controlled signal messages can be accepted in the opposite (inward) direction. In the case of physical protection system the two-way data flow is allowed, but towards level 2 only controlled data flow to the extent necessary for operation and fulfilment of function can be allowed.

b) Remote maintenance access is not allowed.

c) Physical connections to the systems should be strictly controlled.

d) Vulnerability assessment involving actions on the systems may lead to plant or process instability, and should therefore only be considered using test beds, spare systems, during factory acceptance tests or during long planned outages (nuclear safety aspects are included in other regulations).

3.3.2.5. Specific measures for protection level 1

In addition to the measures relevant for the generic level:

a) No networked data flow of any kind (e.g. acknowledgment, signalization) from systems in weaker protection levels should be authorized to enter level 1 systems. Only strictly outward communication should be possible. Note that this kind of strict one-way communication does not ensure reliability and integrity natively. Note also that this excludes any sort of ‘handshake’ protocols (including TCP/IP), even with controlled connection directions. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and risk analysis.

b) No remote maintenance access is allowed.

c) Physical access to systems is strictly controlled by the licensee.

d) The number of staff given access to the systems is limited to an absolute minimum.

e) The two person rule is applied to any approved modifications made within the computer systems.

f) Licensee should log and monitor all activities.

g) Every data entry to the systems is approved and verified on a case by case basis (item a) forbids data transmission to an external network).

Organizational and administrative procedures should be developed for any modifications, including hardware maintenance, updates and software modifications.

3.4. Developing the protection plan of programmable systems and components

The protection plan for programmable systems and components is a key document for the implementation of the protection program.

The protection plan of programmable systems and components must include the systems to be protected, their protection level and specific protection measures, the organization responsible for implementing the protection measures and in case of critical programmable systems and components the organization responsible for ensuring continuous operation. The protection plan must include provisions for the education and training related to protection.

The protection plan documents how the protection objectives are achieved and maintained. It is therefore a live document which needs to be reviewed, modified and approved regularly. The protection plan should document the manner and frequency of the revisions, maintenance and approval. The protection plan of programmable systems and components –as part of the physical protection plan- must be in line with the provisions of the physical protection plan, as several protection control measures are related to physical protection and vice versa. Due to the variety of confidential information relating to the protection of programmable systems and components, the documents of the protection plan must be structured and classified according to the confidentiality of their content, and the access to the various parts must be determined according to the confidentiality of the information.

3.4.1. Inventory of systems (systems, networks, applications and their interfaces)

The facility must have an up to date inventory containing a comprehensive list of all programmable systems and components. The asset inventory of programmable systems and components should be compiled such a way that it incorporates all relevant information and data for completing the risk assessment. This asset inventory should be updated on a continuous basis

to ensure its up to date status. The asset inventory of programmable systems and components should include at least the following:

a) A list of programmable systems and components (manufacturer, type, properties),

b) operation model, function and task of programmable systems and components,

c) list of applications running on the systems (operating system, software, programmes and services),

d) interfaces and network of systems and components including electric power supply of systems,

e) networks diagram (topology and topography), including each external and internal interfaces (IP addresses, MAC addresses etc.),

f) analysis of data interfaces and data flow to identify the systems communicating with other systems or devices,

g) the processes and operations that trigger communication between systems, the characteristic of communication and the protocols applied,

h) location and placement of programmable systems and components.

In the course of establishment of asset inventory of programmable systems and components and during the risk assessment it should be kept in mind that both the inventory itself and the data and information collected as a result of risk assessment can be sensitive from protection point of view for the licensee. Appropriate protection or qualification as necessary should be provided for them.

Compiling the list of the programmable systems and components takes place in the framework of the configuration management. The protection plan must also address the way in which the programmable devices can be identified.

Configuration management ensures consistency between the design base, the plan and the implemented system. For this purpose, it must contain all the information and data to check consistency. The introduced system is a system that meets the testing and control procedures and therefore also meets the protection requirements. The task of configuration management is to record this protection status of the programmable systems and components as a basic configuration together with the pre-configuration (see 3.4.1.1), and to maintain the protection status by ensuring that changes are carried out in a controlled manner.

3.4.1.1. Basic configuration

To develop the basic configuration the following steps should be taken:

a) A system for recording the components of the programmable systems and components must be established. The records must reflect all authorized system component and must be developed so as to include all the typical data and information required to carry out the risk assessment.

b) The records must be supported by automatic mechanisms that are capable of detecting new, not yet recorded components and the entries of removed components.

c) A basic configuration of the programmable systems and components must be set up.

d) The basic configuration should also be set up for the developer and test environment in addition to the operating environment.

e) The basic configuration and should be maintained in conjunction with any changes, for which automatic mechanism should be used if possible to ensure the consistency of information.

f) Access to the configuration management system should be limited and only those with proper qualification and authorization should be allowed to make changes. Every change should be logged. The consistency and accuracy of the data should be monitored regularly through internal audits.

g) Configuration changes to programmable systems and components must require strict physical and logical access. Access must be logged and the logs must be checked regularly, preferably through automatic mechanisms. If access restriction cannot be done through automatic mechanisms, substitute mechanisms should be used (e.g. physical restrictions, monitoring physical access, employing trusted staff, verifying changes at a later date).

h) Mandatory configuration settings must be defined for the programmable systems and components. Protection settings must be set to the highest level that is compatible with its function. All exceptions must always be documented and justified. Automatic mechanisms should be used that allow the setting and controlling of configuration from a central location.

The asset inventory developed for the programmable systems and components must contain the programmable systems and its components as configuration elements, with a clear identifier, and at least the following information related to each configuration element:

a) Product description (e.g. manufacturer, type, version),

b) Software (e.g. operation system, applications, services) and updates,

c) Disabled or turned off access possibilities,

d) Physical location, localization,

e) Operational model, function and task,

f) Network diagram (topology and topography), including all external and internal connections (IP addresses, MAC addresses etc.) and connections, including power supply of the systems, data connections and data flows,

g) Processes and operations that trigger communication between systems, the characteristics of the communication and the used protocols,

h) Design basics, design and development documentation,

i) Test documentation with the test cases and tested configuration,

j) Operating and maintenance documentation,

k) Applied protection controls,

l) Access rights, persons with these rights,

m) Configuration settings,

n) Protection level ,

o) The changes in chronological order (who, what, when, for what purpose).

3.4.1.2. Configuration changes

Any changes affecting the programmable systems and components must ensure that the system level protection requirements are met, otherwise the protective consistency may weaken over time and its risk may exceed the acceptable level. Therefore, modifications should be examined in terms of the impact on the protection and what protection measures may be needed to mitigate the resulting vulnerabilities. The test is a security impact analysis, which must be performed before the changes take place as part of the approval procedure, after the changes took place as part of the Factory Acceptance Test (FAT) and before applying the changes as part of the Site Acceptance Test (SAT).

For the security impact analysis the following steps must be taken:

a) The feasibility of the changes must be examined. By analyzing the system architecture, the systems and system components that might be directly or indirectly affected by the modification must be examined.

Implementation options should be developed and considered, taking into account the effects on function, safety and protection.

b) Identifying vulnerabilities.

c) Risks must be assessed. When identifying vulnerabilities, the risks should be measured. If the expected level of risk is higher than accepted it must either be reduced through new protection measures, or by modifying existing ones, or the changes must be rejected. An increase in the level of risks is permitted as long as it does not exceed the level of acceptable risk.

d) Existing protection measures must be examined. It must be considered whether the modification affects, and if so, how the existing protection measures of the programmable systems and components directly or indirectly affected by the changes.

e) If, during the inspection prior to the application of changes protection issues arise, consideration should be given to implementing new protection measures or to modifying existing ones. Based on this can the changes be approved or rejected.

After the modification of the programmable systems and components an FAT should be performed. During the FAT, at least the following must be verified:

a) As a result of the modification, the original problems have been resolved.

b) The modifications resulted in no adverse effects to the applications, the functions are available and are working as intended.

c) The original security impact analysis was correct and the shortcomings uncovered by it have been corrected as expected.

d) The changes may be revoked.

After the FAT a virus scan must be performed with the latest virus definitions to verify that the programmable systems and components were not infected during the tests. Changes should be documented.

After commissioning, an SAT must be performed, with the latest updates and a virus scan with the latest virus definitions must be performed following the test.

Before applying changes to an operating programmable system and component, it must be ensured that a recovery can be performed if required in accordance with the recovery procedure for the worst case scenario. The steps for putting the changes into operation must be developed taking into account at least the following aspects:

a) In case of changing several systems, the order of changes must be determined. In the case of redundant programmable systems and components, changes must be made to the backup systems first followed by the operating systems.

b) Applying automatic or partially automatic change execution options.

c) The time required for the implementation of the changes and the time available due to the limitations resulting from the shutdown or operation.

d) Ensuring the compatibility of the modified and unchanged systems.

e) Suspending and restoring the changes (point of no return).

f) Inspection and monitoring of the commissioned system.

g) Crieria for stable operation after modification and closure.

Modifications should be carried out and the configuration management system must be updated after the changes have been implemented by recording at least the following data: causes for the change, change identifiers, affected programmable systems and their versions, persons responsible for the modification and the execution, performed test cases and the implementation steps.

3.4.2. Realization of the protection measures

3.4.2.1. Principles of protection planning

The protection aspects of programmable systems, components and networks should be integrated to the life cycle of construction from the earliest phase of design. Accordingly, the security by design principle should be enforced. The application of the highest level of protection by the chosen technology, applied systems, components and solutions should be a primary objective during the design. The protection level of the chosen technology solutions should be uniform and graded to the risk. The protection of the system should be considered and treated with equal weight besides the functionality and reliability of the system.

Comprehensive and detailed risk assessment and evaluation should be conducted during the design and construction of the system, considering the potential vulnerabilities, threats and attack scenarios. The residual risks should be identified and harmonized with the senior management based on the results of the risk assessment conducted in the design phase. The acceptable level of identified residual risks should be determined by the senior management of the facility. The operator, based on the results of the risk assessment, should apply such protection means and control measures in order to protection the system, which can be organically integrated into

the chosen technology, provide protection that is proportional to risks, and thus can reduce the residual risk to the acceptable and as low as achievable level.

In addition to the compliance with the functional requirements, reliability and failure resistant operational expectations, the protection of the three basic requirements of protection should be met during the design and construction of the system. The priority order of the three basic requirements of protection is as follows:

a) availability (continuous and reliable operation, usability and accessibility of the system),

b) integrity (assurance of the original function of the system, protection against corruption of data input, data presentation and data transmission, provision of data consistency and correct information),

c) confidentiality (protection against unauthorized use or interception of the system; protection of functions and data against unauthorized access

The design and construction of the system should be prepared for management of violation of the above protection requirements; appropriate control procedures (means and measures) should be applied for the protection of the system. The types of the applicable control measures are as follows (according to PreDeCO protection design principle):

a) preventive,

b) detection,

c) responding, recovery or correction.

d) The selected and applied protection means and measures should fit to the applied technology and its elements, as well as they should meet the following conditions:

e) closed (considering every potential vulnerability and threat),

f) comprehensive (considering every relevant element),

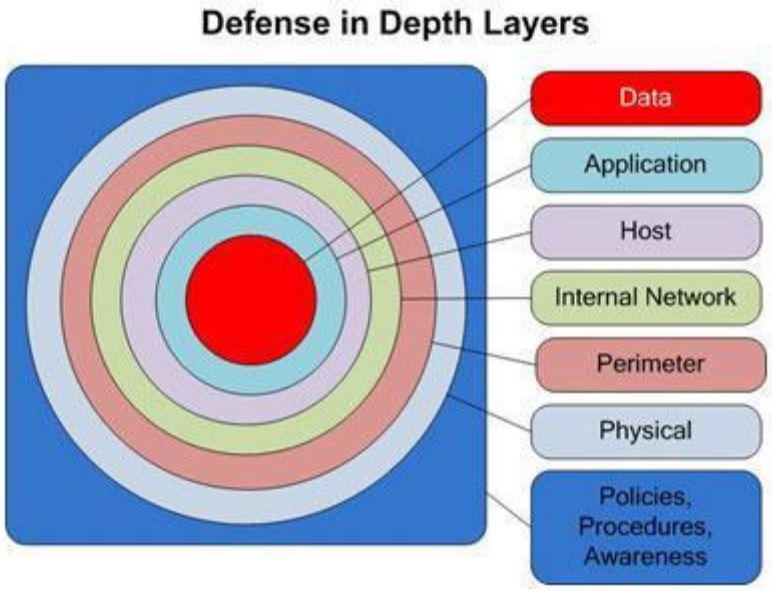
g) continuous (the protection is continuous in time without breaks),

h) proportional to the risk.

3.4.2.2. Defense in depth

The Defense in depth principle should be applied during design of the protection of systems, as well as during selection of the protection means and measures belonging to the components. The defense in depth principle

means that different protection techniques and means are applied in the subsequent layers of the system to be protected, in order to provide appropriate protection of each layer (level) of the system against unauthorized intervention or an attack.



The means and protection techniques applied for the protection of the layers should fit to the elements of the chosen system, and should provide protection proportional with the risks in each layer. The protection techniques and means applied in the various layers aim at continuously preventing a potential unauthorized access or intrusion through the subsequent layers, requiring more time, more technical expertise, more special attack technique and more complicated means. The protection solutions to be applied in the different layers are described in detail in the next sections.

3.4.2.3. Regulations, procedures and training

The computer protection of the system is provided by the complete set of administrative and personal protection measures and procedures. The operator should present all those documents, which describe the expertise needed for the safe and secure operation and use of the system, as well as the education and training of the operatory, maintenance and user personnel.

3.4.2.4. Resistance to environmental conditions

The system components, data transmission devices, host measurement data collectors and the outside means should operate as parts of a

distributed network, at different locations of the facility, placed far from each other. The data collectors and data transmission devices placed at various locations of the facility should reliably work under totally different environmental conditions to assure the required level of availability of the system. Accordingly, the exposure to potentially harmful environmental conditions should be considered during the design and construction of the system and the distributed network.

An important aspect during the selection of the components is that these components should resist the extreme environmental effects characterizing the place of installation. Such environmental conditions are:

a) Extreme temperature (very high or very low),

b) High humidity, dust or vibration,

c) potential mechanical damages or presence of chemicals,

d) high electromagnetic interference (EMI), radiofrequency interference (RFI) and electromagnetic disturbances (EMC).

3.4.2.5. Physical access protection Fizikai hozzáférés védelem

The operator should specify and then establish those physical access protection solutions, which can prevent the potential of unauthorized access. The proper localization of the devices should assure that they can be only accessed in a controlled way exclusively by the operation, maintenance personnel. The following solutions can be applied for the physical access protection:

a) Placement at a physically protected, guarded area (behind fence, gate and guards),

b) Placement in lockable buildings and rooms that are equipped with access control system,

c) Placement in buildings equipped with camera observation and alarm system,

d) Placement in special, lockable cabinet (rack-cabinet).

3.4.2.6. Network perimeter protection

The operator should clearly separate the internal (protected) network of the “secure” technology system from the “non-secure” external network (e.g. company informatics/management network or the network of an external client) by the establishment of one or more, but accurate and well defined

"perimeter line". The fundamental objective of the application of perimeter protection means is to prevent any unauthorized connection between the two networks and to control (allow or block) the connection and data transmission of the networks and network devices. The operator should separate the internal, secure network to protect from the external, unreliable network by the application of perimeter protection devices, in order to assure that only permitted data transmission may flow between the two networks. In addition, the structure of the inner network should be hidden from the devices of the external network, in order to prevent unauthorized access from the external network to the devices of the internal network. The devices that are applicable for network perimeter protection:

a) Firewalls, demilitarized zones (DMZ) – only for low risk,

b) virtual private networks (VPN) - only for low and medium risk,

c) gateways – for medium risk,

d) physically unidirectional data diode – preferred solution for high or elevated risk.

3.4.2.7. Technical and logical access control

The technical and logical access control includes all those technical protection measures installed and applied in devices, which controls the local logging in as well as the remote access (e.g. access to the administrator or management interface) in logical and technical ways, and reduce the risk of unauthorized access. The available technical and logical protections installed in devices should be implemented on an appropriate level. Such protection solutions are:

a) Block of unused input and output (I/O) ports and connectors

b) Association of the ports and connectors of network devices (MAC address filtering), automatic blocking of the port in case of a violation (port security settings),

c) Control of access to the administrator and management interface of network devices (IP address filtering),

d) Authenticity procedures (identification of users, password protection) for local and remote access,

e) Role based access control (RBAC) for local and remote access.

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

When designing programmable systems and components, the plans must show the access options (services, ports) planned for the programmable systems and components, and their needs must be justified. Access options may be required for normal operations, maintenance or in the case of emergency. Thus, the access options must be assigned to functions.

Manufactured programmable systems and components must demonstrate as part of the FAT that they are free of unnecessary access options. This certificate must be attached to the construction license application. For this, before performing the FAT, unnecessary access options must be removed and/or switched off. The necessary and the removed or turned off access options must be documented. The latest updates must be installed on the programmable systems and components after testing and checking them. During the FAT testing procedures must be carried out to verify that access to the programmable systems and components is in accordance with the documentation.

Installed programmable systems and components must be verified as part of the SAT that they are free of unnecessary access options. The certificate must be attached to the operation license application. The latest updates must be installed on the programmable systems and components after testing and checking them. During the SAT testing procedures must be carried out to verify that access to the programmable systems and components is in accordance with the documentation.

During operations regular checks should be performed to ensure that unnecessary access options to the programmable systems and components are consistent with the configuration management register. The integrity verification of the Reserve and test programmable systems and components and during maintenance on-site systems must be ensured (e.g automation must be used for integrity checks (HIDS)).

3.4.2.8. Protection of internal networks

In addition to the establishment of the network perimeter protection, the application of the defense in depth principle requires the control and supervision of the internal (secured) network flow of the devices. The application of devices serving for the protection of the internal network can prevent or timely detect the attempts of accesses to the internal network, the undesired or extraordinary network flow (e.g. proliferation of worms, viruses and other harmful programs) and the unauthorized network activities.

The lonely application of the network perimeter devices (perimeter protection) cannot be considered as sufficient protection. If the firewall is by-passed, then an unauthorized access, an attempt of an attack deploying the vulnerability of the firewall or any other extraordinary network flow can be detected by observing and controlling the data flow of the internal network. The use of internal network protection devices should not be limited to the detection of attacks or attempts to access from remote networks, but their other important areas of use are the timely detection and prevention of attacks initiated in the internal, secure network, as well as the detection of internal abnormal network flow.

Special, industrial communication and data transmission protocols (e.g. Profibus, Fieldbus, Modbus, DNP, DNP3, ICCP) are widely used in the environment of technological systems as well as in their internal network; they provide the unified data communication between the network devices (e.g. IEDs, PLCs, RTUs, data collectors, hosts and SCADA/DCS servers). At the time of their design and construction, the primary requirement for these industrial network protocols was the fast (real time) and reliable data transmission, while these protocols were found to be weak and vulnerable from network and computer protection viewpoints. This issue needs to be resolved by the management of the internal network protection risks of technology systems.

Consequently, an important requirement for the design of technology systems' network and selection of network devices is the application of newer, secure protocols and devices compatible thereto, instead of old, weak and vulnerable industrial communication protocols. The means that can be applied to protect the internal network are as follows:

a) establishment and use of secured communication protocols (e.g. IPv6, SSCP, SSL/TLS, SSHv2, HTTPS, IPSec, SNMPv3),

b) coding of network communication and data transmission (use of coding from host to host, if appropriate),

c) identification and authentication of network devices and equipment (e.g. RADIUS server, EAP CHAP),

d) observation and monitoring of network data flow (event logs, alarms)

e) application of Network Intrusion Detection Systems (NIDS).

3.4.2.9. Protection of servers, workstations and HMIs

The highest possible protection settings, configuration and parameters should be performed (i.e. *system hardening*) on each server, workstation and operator HMI (*host*) device, and additional technical and software based solutions should be applied for the protection of the hosts. The techniques and tools that are applicable for the protection of the hosts are as follows:

a) Enhancing the protection of operating systems and software running on servers and work stations (system hardening),

b) removal or blocking of unused, unnecessary programs and services,

c) removal or blocking of unused, unnecessary accounts (e.g. Guest account),

d) change of default user accounts and passwords,

e) modification (further limitation) of file system level access to operating systems,

f) blocking or limitation of input/output ports (blocking of serial ports, USB ports, CD/DVD devices, password protection of BIOS, etc.),

g) Host-based Intrusion Detection Systems (HIDS) for the integrity check of servers and work stations,

h) software based protection against the intrusion of harmful program codes (malware), application of integrated antivirus software,

i) application of heartbeat signals, i.e. a device monitoring and indicating the actual operational state and communication links of the system,

j) updating of operating systems, applications, software and device controlling programs (continuous and periodic security and software updates),

k) application of a unified and standardized hardware and software environment, application of complex “image” installation kits.

3.4.2.10. Protection of applications and running programs

In addition to enhancing the protection of server and client operating systems applied in technology systems and of the running environment (i.e. system hardening), the highest possible protection of application and software performing system functions (independently of whether they are uniquely developed or commercial box software) should be provided. Built-in inner devices serving for the protection of the applications and software, as well as external technical solutions should be applied. The means and

measures providing protection of the application and programs are as follows:

a) Blocking, removal or modification of default user accounts,

b) Supervision of user accounts of the application (identification, check of authorization, password management, logging),

c) Role Based Access Control (RBAC), use of ID and password in applications,

d) Reliable work session and connection management (Session Management), application of SSL and SSH,

e) Logging of actions, tracing and auditing of user actions.

3.4.2.11. Protection of data

The protection of the data stored and managed in technology systems is inevitable for compliance with integrity and availability requirements. The system should be provided with appropriate (host to host) protection on the data storage, management and transmission level. Since the protection of the data stored and managed in the system is in close relation with the protection of the applications and software, thus the protection informed program design and development is a fundamental expectation. The following aspects should be highly considered during protection informed program development.

The entire system as well as all of its software components should be designed and develop in a way that provides protection against the following attack scenarios:

a) Attack inducing buffer-overflow,

b) Man-In-The-Middle type attacks,

c) Denial of service type attacks (DoS and DDoS),

d) In addition, the web based applications should be protected against the following is;

- SQL-injection, command injection,
- path/directory traversal,
- Cross-Site Scripting – CSS/XSS, CSRF,
- Remote File Include – RFI, File Upload,

In order to comply with the above requirements, the following conditions should be met, as a minimum by the software applied in the environment of the system:

a) Checking and filtering of every input – only valid and validated data should be accepted,

b) only data of pre-defined type, format and characters should be accepted,

c) the data input should be protected by coding against unauthorized modification,

d) calling and use of stored procedures for databases,

e) the user identifications and passwords should be stored in a coded format (i.e. never as a plain text) in programs, data or databases,

f) the important and critical data should be stored in coded format,

g) such program languages and program development tools should be used, which (after translation) result in automatic and secure memory management during the running of the program development tools,

h) host to host authentication should be used, as appropriate; integrity checking mechanism should be applied in data transmission between processes and during communication,

i) the program or the source code should not include passwords or code-keys as plain text; they should not be transmitted without coding in the network,

j) developer frame systems supporting complex program and software design and development should be applied,

k) automatic source code revision, or source code analysis tools should be used.

3.4.2.12. Assessment and management of well-known vulnerabilities

In the case of each (hardware and software) component and element of the programmable systems, the published and well-known vulnerabilities available in various databases should be identified; the results of this assessment and the management method of these vulnerabilities should be documented. Such open databases are listed below:

a) http://nvd.nist.gov/

b) http://osvdb.org/

c) http://www.kb.cert.org/vuls

d) http://www.securityfocus.com/bid

e) http://tech.cert-hungary.hu/vulnerabilities

For up-to-date handling of vulnerabilities, a continuous communication link should be established between the Constitution Protection Office, the Information Office and possibly the internal CERT institutions of the organization. The order of contact must be regulated.

3.4.2.13. Program updating and installing patches

The actual program updates and security patches officially published by the manufacturers of the system components should be installed on each hardware and software components and elements prior to on-site acceptance. This relates to the firmware of the hardware devices, as well as to the operating systems and technology software. The *Site Acceptance Test* should be conducted only after the installation of the program updates. It is probable that during the service life of technology systems the software and hardware manufacturers will periodically publish newer program updates and security/safety patches, which aim at correcting the errors or security threats/risks recognized in the meantime. Consequently, a Program Update and Security Patch Management guideline should be elaborated for the entire technology system, according to which the operator personnel should preserve the required level of computer protection.

The periodically or regularly conducted vulnerability assessment or the incident management report may contain vulnerabilities that need to be corrected or reduced. As a result of the risk analysis, new protection measures may also be required. Monitoring and analysis of the systems' performance may also reveal gaps in functions, protection or safety that need to be repaired or incidents may become known where countermeasures are required. The vendor may also issue security updates, so it is important to ensure that this information is available on time (e.g. through contractual agreement or security update monitoring) to avoid zero-day attacks.

Security updates available this way should be considered as changes and therefore must go through the life cycle of programmable systems and components from design through acceptance tests to commissioning and relevant licensing procedures. In this regard, each programmable system and component must be handled separately. The security update procedure for programmable systems and components must be prepared. The procedures must be defined in such a way as to minimize the safety and security risks arising from or relating to the security updates. To this end, the policy must include verification and validation tasks for security updates, specific approval procedures, or special authorization requirements and audit supporting steps. Among the verification and

validation tasks related to the modification is the protection impact analysis and the related risk analysis. The procedure must be consistent with several other procedures, most important of which are the configuration change, configuration management, risk management, incident management and recovery management.

The need to perform the update must be decided on the basis of a risk analysis. If the level of residual risk of the programmable systems and components is unacceptable without the update, the update must be applied. Otherwise there is a possibility of weighing. Applying the updates in a controlled manner must take place within the context of configuration change management, taking into account the following:

a) In the case of a general vendor security update the required version must be accurately identified but it is also worth checking what other updates are available.

b) The security update conditions must also be examined e.g. how to prepare the system, whether other updates are required prior to the update etc.

c) The security update must be obtained from a trusted source and the identity, integrity and documents must be verified

d) In the case of a specific security update, the software must be prepared according to the system design and development rules and it must pass the acceptance test.

e) The obtained security update must be virus scanned. Based on the documents it must be ensured that the security update can be performed.

f) Before the FAT the current and verified security updates should be installed on the programmable systems and this must be documented.

g) Before the SAT current and verified security updates should be installed on the programmable systems and this must be documented.

For programmable systems and components the security update procedures must be prepared prior to the first FAT. Because security updates change the programmable systems and components, and the means of obtaining, storing and other particularities may change over time the security update procedures must be maintained to keep track of the changes. Thus, the policy for security updates is a live document that must be registered in the configuration management system and its versions must be tracked together with the security updates it performs.

The purpose of the risk analysis required for the modification is to demonstrate that the risk of the system does not exceed the acceptable

level as a result of the modification. Should the level of risk exceed the acceptable level, risk reducing protection controls are required. Because of all this, modifications must be made in the framework of the configuration change procedures.

During the risk analysis, it is necessary to examine the feasibility of loading the configuration settings, parameters and date from the old programmable system into the new programmable system (migration). It must be ensured that the old date are accessible, can be copied, complete, compatible with the new system and whether the data transformation is necessary.

Any change to the programmable systems and components is considered to be a modification and must go through the FAT, construction license application, SAT and the operating license application.

3.4.2.14. Protection against electromagnetic impulses

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

Protection of programmable systems and components against very fast electromagnetic impulses must be designed and constructed in accordance with the physical protection of the facility and the defense in depth strategy. Fast electromagnetic impulses pose a threat to programmable systems and components and consequently risk assessment should be performed to assess the threats' impacts and probabilities on them, after which the protection control measures must be developed based on the tolerable level of risk. The sources of threats to the protection are the harmful electromagnetic impulses that can also be artificially generated. The integrity and availability of the data and the programmable systems and components must be protected against their effects. Consideration should be given to the protection of data networks, electricity supply systems and cooling systems.

In the risk analysis the conductive and inductive effects transferred by the cables and the effects of the electric fields must be analyzed. Protection against the adverse effects is physical and it is recommended to protect the systems by zones. Because in defense in depth, the zone boundaries are also physical boundaries, it is recommended to fit the two protection zones together. This way, to ensure the protection level assigned to the protection zones the threats posed by electromagnetic impulses must also be taken into account. The applicable protection control measures are as follows:

a) Grounding and equilibrium potential.

b) Magnetic shielding for programmable devices and cables.

c) Trail design for cables.

d) Coordinated surge protection for programmable devices, cables and cable endings.

Malicious attacks that cause electromagnetic impulses can be prevented or their effects reduced by restrain through physical boundary protection. Therefore, in defining the physical boundaries of the defense in depth, such attacks should also be considered.

The planned protection control measures must be documented in the protection plan for programmable systems and components in accordance with the physical protection plan.

In the case of operating facilities, it is also necessary to examine the protection of the control rooms, and if necessary to install shielding solutions (grounded, suitable mesh nets).

3.4.2.15. ID and password management

In order to identify, persons and systems must be provided with their own unique IDs and the designation has to be approved. The IDs and their access have to be logged in the registry and in case of withdrawal of those access privileges the registry has to be updated.

Accesses should be appropriately validated to suit the level of protection of the programmable system so that it cannot be easily bypassed or hacked. In most cases the authentication is done by passwords, therefore, the issuance, communication and use of passwords have to be regulated. The goal is that the password is strong enough and only the person whom it belongs to knows it, so that it unauthorized persons will not find out.

In addition to the password protection other security measures can also be defined that may substitute or complement the use of passwords. These can be for example biometric authentication (retina, fingerprint, iris, voice), chip cards and tokens. In such cases the advantages and disadvantages of the authentication method as well as the application conditions should be taken into account. If required by the protection level, multi factor authentication is required. In such cases, usually multiple authentications are performed one by one and each authentication must be successful for validation.

Authentication, whether successful or unsuccessful is an event that must be logged by the programmable systems and irregularities must be reviewed within the framework of the incident management. In addition to people, in many cases, services running on the programmable systems must also be identified and authenticated. This may be done in a fashion similar to

people, such that here the credentials are typically a coded password. It is important that the minimum eligibility principle is applied also to services.

In addition, authentication and verification of messages and electronic documents may be required. In these cases the messages must be digitally signed and the public key infrastructure (PKI) must be established between communicating systems to handle private and public keys. For this purpose, appropriate protocols (e.g. IP Sec, SSL/TTL, S/MIME) and supporting applications must be used. The internal issuance or acquisition of digital certificates and their protection must be regulated by procedures.

3.4.2.16. Use of portable devices and mobile storage devices

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

Portable devices, including mobile storage devices and proprietary Bring Your Own Devices (BYOD), are capable of revealing confidential data, transmitting infected codes to programmable systems and components, as well as booting up systems by exploiting their operating systems. Therefore, their use should be limited by administrative, physical and technical control measures, taking into account the following:

a) The use of all portable devices must be prohibited unless authorized (white list). It must therefore be determined who can use what, where and with what.

b) Entry of BYOD devices to the protection zones shall be prohibited.

c) Movement of portable devices between the protection zones shall be prohibited.

d) Monitor, log and control the connection of portable devices to the programmable devices.

e) Physical data movement by portable devices must be limited in time and space (when, where) through physical access protection control measures.

f) The integrity and confidentiality of the portable devices must be ensured at the same level or protection as the connected programmable devices.

g) The origin of the portable device and the integrity of the data contained therein must be ensured. The origin and owner of the data must be checked and the identity of the data source must be verified to ensure that the source is indeed the one they are claiming to be. Furthermore, it must be checked whether the data remained intact during transport.

h) Connectivity points for portable devices on the programmable systems and components must be reduced to the minimum necessary and as far as possible the connectivity duration must be limited.

i) The boot function of portable devices must be turned off or removed from the programmable systems.

3.4.2.17. Wireless devices and networks

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

The spread of wireless devices and networks is becoming more important among programmable systems and components. Use of the technology is in some cases advantageous (e.g. lack of wired network, providing alternative means of communication) but its use should be considered in terms of protection:

a) Radio waves can cause loss of communication.

b) Unauthorized interception or blocking of the channel poses a risk.

c) Encryption, authentication, intrusion detection is required.

d) Encryption mechanisms and protocols change rapidly.

e) All effects on safety and security must be considered.

f) Separating the network from the wired network is recommended.

If wireless networks are required, access to them must be limited by protection measures, taking into account at least the following:

a) Their use must be prohibited in the case of programmable systems and components and should only be permitted in certain justified cases.

b) Access area must be limited to the required area and the availability to the required duration.

c) The access function on programmable systems and components must be disabled, if the access is not permitted

d) Available wireless networks should be monitored.

e) Access to networks shall be in accordance with the defense in depth.

f) If possible, cryptographic means shall be used to ensure the authenticity of the data source and the integrity of its content during data transmission (e.g. protection against man-in-the-middle attacks).

The use of wireless networks such as portable devices within the facility must be regulated.

3.4.3. Continuous operation, system back-ups

3.4.3.1. Continuous operation

In the case of safety critical systems, measures should be put in place, which, in the event of an accident or disaster, as well as through problems or errors resulting from operation or usage, can ensure the continuity of operation and if necessary recovery.

Preventive measures have a fundamental role in the maintenance of continuous operation; their main areas are:

a) Establishment of operational and maintenance procedures.

b) Provision of spare components.

c) Provision of well-prepared operating and maintenance personnel.

d) Regulation of security/safety savings.

e) Determination of responsibilities.

f) Consideration of measures aiming at providing external service and external stocks of spare components.

g) Application of physical, logical protection systems and measures.

h) Application of fail-safe technical solutions.

Required regulations to ensure continuous operation:

a) The execution of hardware, software, data and parameter modification in systems and components should be regulated. The modification should always be documented.

b) Rules should be developed regarding virus protection.

c) Rules should be developed regarding portable devices.

d) Recovery plan should be developed for the planned, fast and effective response to failures and transients.

3.4.3.2. Backup of the systems

Purpose of creating backups

In order to ensure the integrity and availability of the safety critical equipment, system or information, backups should be made of the operating system, programs, data, parameters and documents.

In the event of a malfunction, backups make it possible to restore the equipment to a functioning state before the failure occurred, with the least possible downtime.

In order to achieve this, the regulation for creating copies (the record) should list the components to be backed up, the type of copies to be made for each component, the frequency and in what circumstances should backups be made, as well as how the backups should be verified, stored and recorded.

Scope of the regulation for creating backups

The rules for creating backups must be defined as being applicable to all equipment and systems, which are to be backed up on a regular or occasional basis.

The system and all its components to be backed up should be recorded. In the case of any component of a given system, the entire program system should be recoverable from a copy. The method of recovery should be determined in the valid documentation of the component. The reproduction should be performed within the timeframe defined in the relevant operating instructions.

Defining backup categories

The backup policy must prescribe that the backup should be done in at least the following two categories:

a) Professional area backup: such backups should be made for the daily tasks of the maintenance and operator organization in order to respond to unexpected errors and to recover the systems, components and data elements.

b) Reserve backup: reserve backups are made for system recovery purposes in the event of a failure, but are stored independent from the professional area backups. This way the system, data elements can be recovered even in the event of any problem with the professional area backup (damage etc.).

Rules for creating backups

The regulations governing the creation of backups for safety critical systems should be elaborated taking into account the following aspects:

a) Whether the backups should be done at predetermined, cyclical intervals.

b) Whether a copy should be created prior to the planned maintenance or modification of the system.

c) Whether a copy should be created following the maintenance or modification.

d) Whether the entire system should be copied or just the scope affected by the modification (system component, database, etc.)

Regardless of the reason for creating a backup, the fact that a backup was made should be documented in all cases. The copies should be clearly identified and registered.

Storage of backups

In the regulation governing the backup creation of safety critical systems, provisions must be elaborated for the storage of the backup. In doing so, the following should be taken into consideration:

a) Backups required for the daily corrective actions of operation and maintenance should be stored in a way that the recovery should be performed as soon as possible if a problem occurs in the continuous operation. The storage location should assure the availability of the copies/saves at any period (i.e. during working hours and before/after them).

b) The workflows of saves belonging to different systems should be stored separately by systems, in order to reduce the likelihood of misuse. Another important requirement is that only the actual version of the workflow should be stored at the location of the system.

c) A reserve backup should be stored in a place that is protected against a damage induced by a common cause.

d) The regulations for storing the copies/saves should provide that only the authorized persons of the operator and maintenance personnel should have access to them.

e) The storage location of the data carrier should be physically protected; in the case of electronic storage (e.g. server designated for this purpose) appropriate authorization process should be in place.

Verification of backups

The regulation governing the backups of safety critical systems must at least contain the following provisions about the verification of backups:

a) How often, in what cases should the verification process be conducted?

b) It should be verified whether the required number of copies are available at the specified storage locations.

c) It should be verified whether the backup IDs are identical to those in the records.

d) The current state of the system should be compared with the last backup. If differences are found (i.e. modification was performed in the

system), the backup should be supplemented and the records should be updated.

e) Determine the measures that need to be taken in the case of failure or non-usability (damage, incompatibility) of the backup is observed.

Reloading backups

When elaborating the reloading section of the regulation governing the creation of backups, it should be determined whether:

a) the documentation of the systems and components should include the re-loading procedure of the backups.

b) Is verification by re-loading required/possible.

Identification, record keeping

In order to prevent potential misuse of the backups:

a) The identification system of the backups should be established. The identification system should clearly refer to the saved system, its location, the time when the backup was created, and the level of the backup (the entire system, software component, database).

b) The recording system of the backups should be established.

c) The person, organization responsible for keeping the records should be identified.

A copy of the records should also be created for such a case when the records become inaccessible for any reason.

3.4.4. Protection related education training, protection culture

3.4.4.1. Determination of the objectives and rules of the protection related education and training

The objective of education and training on the protection of programmable systems and components is to let the participants be aware of the protection needs of the systems and components used by them, and of the measures they should do for the preservation and enhancement of the protection level belonging to the job positions.

It should be regularly checked, based on the education, qualification and/or experience, whether the personnel have the protection knowledge required for their roles. The required protection knowledge should be determined; where possible, qualification and audit programs should be used for checking its up-to-date status.

The effective training of all users (user, advance user, administrator) of programmable (technology and administration) systems requires the identification of the training needs of each user group. Besides the identification of the needs, this process should include the development and implementation of a strategy serving for the effective training and measurement of the results.

Individual training plan should be developed for each user group; the training plan should be regularly updated.

The training programme of new-comers should include the protection knowledge of programmable systems; this expectation should be reflected in the internal regulation.

3.4.4.2. Protection training criteria according to the established levels of authorization considering the requirements of the protection levels

Such training criteria system should be developed taking account of the defined protection levels, which provides the knowledge level that is needed for the compliance with the requirements of the various protection levels.

Protection levels / User rights	User	Advanced user	Administrator
5	I.	I.	I.
4	I.	I.	II
3	I.	II	II
2	I.	II	III.
1	II	III.	III.

Criteria should be established for training categories I, II and III for training of protection of programmable systems, including the frequency, knowledge level and depth, and duration of training, and the methodology of examination of effectiveness.

3.4.4.3. Special educations and trainings

Prior to the introduction of any new technology standard, procedure or product that may affect the protection of the programmable systems and components to the facility, training program must be developed regardless of the purpose of the purpose of their introduction.

The training should be tailored for managers, operators and maintenance personnel, and for protection and operational roles. It is advisable to include theoretical and practical elements in the training. It is advisable to deepen the acquired knowledge through practical trainings (declared or ad hoc).

In addition to the established training courses, if necessary extraordinary training should be conducted.

3.4.4.4. Development of the protection culture

The development of the protection culture of programmable systems is such a continuous and important activity, which may result in a favorable state meeting the following conditions:

a) Every user must participate in training on ethical code of conduct and system protection awareness. Positive attitude should be observed regarding ethical behavior and system protection principles.

b) Each user should get appropriate level of training on system protection procedures aiming at preventing harms induced by failures of availability, confidentiality and integrity.

c) The management should keep an eye on the appropriateness of the education and training programmes by their continuous revision and actualization.

d) Practical training should be provided at regular intervals to management, operators and maintenance personnel in order to make everyone aware o the importance of protecting the programmable systems and components.

The most effective way of preventing man-made intentional or unintentional damages is by establishing an organizational body responsible for the protection of the programmable systems and components, defining roles and responsibilities and by restricting access. These should be supplemented by protection measures related to the staff or programmable systems and components handled by the staff, which shall include at least the following:

a) Prospective employees should be vetted before hiring, which includes checking the following: prior violations, correctness and completeness of resume, references, psychological behavior, internet and other media presence.

b) Staff members with access to high protection level devices shall be subject to more stringent and regular checks. In some cases, in keeping with the privacy rights, the behavior and work of the staff shall be monitored following the provision of access rights.

c) Management of the programmable systems and components must be designed to minimize human error and take into account the reaction time of humans.

d) Information input, including manual data input and data readings should be limited as far as possible and the completeness, accuracy, validity and authenticity of the data entered should be verified by the programmable systems. Verification should be performed as soon as possible i.e. during data input or directly after data input, but before saving or processing. If validation ranges can be determined then the validity of data entered should be examined. If possible, the consistency

of the data being entered should be checked against each other and against previously entered data.

e) When displaying information, clearness and visibility should be sought and only the necessary amount of information should be displayed.

f) The supplier must disclose means to prevent the disclosure of confidential information known to employees, which may lead a reduction in the protection of the programmable systems and components.

g) The supplier must communicate within a specified period of time if a staff member with confidential information relating to the protection of the programmable systems and components quits or changes position.

h) The supplier shall provide detailed documentation about the support and maintenance of the protection of the programmable systems and components in the event that the business relationship with the supplier is terminated.

i) The supplier shall return all confidential data when the maintenance of the delivered programmable systems and components is completed.

j) The supplier is required to document the security measures applied to the staff members of the entire supply chain, vet the staff members and to monitor their behavior and compliance with the security measures.

k) The contracts of suppliers involved in procurement must clearly and in detail include the security measures concerning staff members.

If, despite the preventive measures damage does occur, it shall be considered a protection incident for the programmable systems and components and is subject to the recommendations and procedures of event management (see 3.4.7). However, due to the staff nature of the attack and damages, incident management can have several special measures. These may include for example the need for containment, the need to stop the damage or the need to provide evidence. These may require special procedures that must be documented.

3.4.5. Protection review

The purpose of reviewing the protection measures is to verify their operation, effectiveness and compliance with the requirements.

The most important method of the review is the self-assessment. During self-assessment the leader of protection and the protection officers should comprehensively and systematically verify the compliance with the protection plan. A general assessment is made on the operation of the protection measures of the facility; in addition, they formulate recommendations on the necessary modifications and developments.

The senior management is responsible for the regular evaluation of the findings of the self-assessment, and to establish measures for the necessary modifications.

The protection of the programmable systems of the facility, the protection plan, the execution of the protection measures described in the protection plan are regularly reviewed by the Authority through announced and unannounced inspections.

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

The implementation of the protection controls must be designed so that their correct operation can be verified. To do this, the events for which logs are to be generated must be specified. The content of the logs must be specified and a timestamp of each entry must be recorded. Care should be taken that enough storage space is available to store the audit logs and access to the files must be restricted. If necessary, the logs can be copied to non-modifiable media, and consideration should be given that if needed the logs can be used as evidence in legal proceedings.

The review should be planned and the scope, aim and checklist should be recorded in the review plan. During the review related documents (policies, procedures, recommendations, logs, access lists, configuration files etc.) should be reviewed, staff should be interviewed and the systems monitored (configuration management, protection procedures, access controls, separation of powers, event monitoring, network architecture etc.). Finally, the results of the review should be summarized in a report. Corrective measures for non-compliance should be formulated and implemented in a planned manner and the implementation should be verified.

3.4.6. Change management in connection with the protection of systems, lifecycle

The protection plan is prepared by the leader of protection, approved by the senior management, who should also make the plan implemented. The protection plan should be annually revised by the leader of protection;

he/she should inform the senior management on the necessary modifications.

In addition, the protection plan should be revised if the lessons learned from events verify or in the case of relevant change in the threat.

3.4.7. Event management

The protection plan for the programmable systems and components must include rules for handling, classifying, preventing and resolving events, and for reducing the damage resulting from avoiding or the occurrence an incident.

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

The behavior of the programmable systems with protection controls must be monitored in order to detect abnormalities as soon as possible.

The protection event management contained in the protection plan includes gathering, filtering, sorting (abnormalities, warning, information) responding and storing of events.

Abnormalities and warning need to be further analyzed and if the protection result is a protection incident, it must be handled.

The process of incident management includes preparation, detection, analysis, containment, elimination, recovery and closure. The purpose of the process is to provide organized responses to minimize the anomalies occurring in the functioning of the programmable systems and components.

3.4.7.1. Investigations, investigative measures

The facility's protection officer will develop the process for investigating the events.

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

Preparation:

Incident management procedures must be developed allowing for quick and organized responses. The procedures must be carried out by the incident management team by performing their determined roles. Procedures must be developed, documented and approved according to the severity of each incident.

Detection:

Automatic mechanisms are essential for the timely recognition of protection incidents. The most important of these are the Intrusion Detection Systems (IDS, Host Intrusion Detection System HIDS), traps (Honeypots, Honeynets) and Security Incident Event Management (SIEM) applications.

There are several signs that may point to abnormalities that need to be monitored. For example a full log file, antivirus or IDS alarm, turned off antivirus software or other control device, unexpected updates, connection to an external IP address, interest in system information, unexpected changes in configuration settings, unexpected system shutdown, unusually high network traffic, unusually high CPU usage etc.

Incidents must be reported after detection. The manner and the way of reporting should be documented in the incident management procedure.

3.4.7.2. Response action plan

As part of the event management, the facility's protection officer is responsible for developing appropriate measures for the severity of each event class.

Additional recommendations in the case of the construction of new nuclear facilities are as follows:

It is necessary to develop regulations and plans for the implementation of the appropriate measures for the following steps:

Analysis:

A prerequisite of being able to analyze an incident is sufficiently available information. Therefore logs and other reports should be configured accordingly. The results of the analysis include among others: the type of the incident, the protection features of the attacked system, timing, circumstances of detecting the incident, attack vectors, attack complexity, antivirus database model, determining physical access method, the method and extend of data corruption and the occurred or possible consequences of the damage.

Isolation:

Once sufficient information is available the incident must be isolated, contained (quarantined) so that it cannot spread further. The containment procedure must be carefully developed, observing the following:

a) The criteria for containment must be clearly documented in order to expedite the decision of its use.

b) The effect and consequence of the containment on the operation must be considered.

c) When deciding on the means of isolation, consideration must be given to the possible damage to resources, the need for preserving evidence, availability (e.g. network connections), required time and resources, the efficiency of the containment (full, partial) and the duration of the containment.

d) It should also be noted that the isolated malware can cause further damage in the isolated system.

e) Isolation can be achieved by manual procedure, automatically (e.g. antivirus), by disabling services or by severing connections.

Elimination:

The malicious code or other harmful resource must be eliminated and it must be ensured that the risk of damage and attack is no longer present.

Recovery:

Examining the exploited vulnerabilities should help identify their deficiencies, and steps must be taken to correct them or reduce their effects through scheduling that ensures that the recovered system is protected and at the same time restoration is completed as soon as possible. Until complete restoration the programmable systems and components may be partially restored if it can operate in island mode and the damage has been eliminated. Remedial measures to be considered may include inter alia:

a) Supplementing the shortcomings of existing protection measures.

b) If an event occurred against which there was no protection in place, new protection measures must be introduced.

c) Modifying the device and installing newer devices to prevent similar damage.

d) Improving the procedures and administrative protection procedures and introducing additional checkpoints.

e) Correcting the operational manuals and other documents.

f) Staff training in relation to the event.

In order to recover the programmable systems and components, recovery procedures must be developed. Backup must be made of all data required for the recovery of the programmable systems and components and the recovery process must describe the recovery steps for each system. The availability, integrity and restoration of the saved data must be assured and confidential data should be treated with the same level of confidentiality as if it were in the operation system.

Data must be saved with a backup strategy to meet the Recovery Time Objective (RTO). Data should be saved with such frequency as required to meet the Recovery Point Objective (RPO). If necessary alternate data storage space must be created that is located at an appropriate distance from the primary one.

Malfunctioning or non-operational programmable systems and components must be restored according to the recovery procedure using the backup. When restoring to a safe and protected state, at least the following should be performed:

a) All system parameters should be set up (to default or specific value).

b) Security patches should be installed and security configurations must be restored.

c) Operating system and applications should be installed and properly configured.

d) The latest available data should be loaded and the proper functioning of the system must be tested.

After recovery, a report should be compiled about the incident and the incident management, which must be sent to the HAEA.