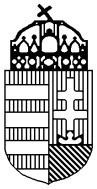
Hungarian Atomic Energy Authority



Guideline 3.5

Design requirements for nuclear power plant electric, instrumentation and control systems and components

Version:

2

2006 July

Issued by: József Rónaky PhD, director-general
Budapest, 2006 July

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

PREAMBLE

The legal hierarchy of nuclear safety regulations in Hungary is as follows:

1. The uppermost level is represented by the Act CXVI of 1996 on Atomic Energy (Atomic Act).

2. The next level basically consists of two government decrees issued as executive orders of the Atomic Act. The 114/2003. (VII.29.) Korm. government decree defines the legal status of the Hungarian Atomic Energy Authority (HAEA), while the 89/2005. (V.5.) Korm. government decree specifies the HAEA's generic procedural rules in nuclear safety regulatory matters. The nuclear safety code consists of seven volumes, which are issued as the annexes of this latter decree. The first four volumes address the NPP, the fifth one the research and training reactors, whilst the sixth volume addresses the spent fuel interim storage facility. These six volumes determine the specific nuclear safety requirements, whilst the seventh volume contains the definitions applied in the code. The regulations are mandatory; failing to meet any of them is possible only in those specific cases that are identified by the decree.

3. The regulatory guidelines constituting the next level of the regulatory system are connected to one of the volumes of the code. The guidelines describe the method recommended by the proceeding authority for meeting the requirements of the nuclear safety code. The guidelines are issued by the director general of the HAEA, and they are regularly reviewed and reissued based on accumulated experience. So as to proceed smoothly and duly the authority encourages the licensees to take into account the recommendations of the guidelines to the extent possible.

4. In addition to the described regulations of general type, individual regulatory prescriptions and resolutions may also address specific components, activities and procedures.

5. The listed regulations are obviously supplemented by the regulating documents of other organizations participating in the use of nuclear energy (designers, manufacturers, etc.). Such documents are prepared and maintained in accordance with the internal quality assurance system of the user.

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Scope and objectives

The Guideline contains recommendations for the method of complying with the design requirements included in Section 5.3 of Volume 3 of the Nuclear Safety Code, related to safety electric and I&C systems and equipment, and for the content requirements of documents that shall be produced during the design.

The objective of the guideline is, by providing recommendations in relation to the design requirements of electric and I&C systems and components of the nuclear power plant, to make the regulatory expectations unambiguous and hereby facilitate the compliance with the nuclear safety criteria included in the effective prescriptions for the given technical solution.

1.2. Corresponding laws and regulations

The requirements included in 5.053 and 5.054 of Volume 3 of the Nuclear Safety Code issued as specified by Article 4. § (1) of the 89/2005. (V. 5.) Korm. government decree on the generic rules of procedures of the Hungarian Atomic Energy Authority in nuclear safety regulatory matters prescribes the following:

"Control and measurement instruments shall be applied to control the parameters of the safety systems and components during normal operation and anticipated operational occurrences and design basis accident. Special attention shall be paid to those operational parameters and systems, system components, which may influence the fission process, the core cooling, the decay heat removal, the integrity of the fuel element, the primary circuit and the containment, and to those information which are required for the safe and reliable operation of the nuclear power plant.

Every predictable failure, which significantly diverts one or more parameters of the nuclear power plant from the safe values, shall be identified and evaluated in order to prevent the failure or to eliminate its effects."

2. DEFINITIONS

2.1. Definitions

This chapter does not repeat the definitions of Volume 7 of NSC issued as annex of 89/2005. (V. 5.) Korm. government decree.

Active safety component

Intervention equipment of a safety system. Active safety components, e.g. hermetic quick closing valves.

Subsystem

Such unit of a system that has alone the same characteristic as of the system.

Archive

Data set assigning the values of process properties, events and interventions to their time of occurrence.

Safety variable

Physical quantity derived from one or more process variable, the value of which is characteristic of the plant safety, and which is used for actuation of safety operation.

Licensed lifetime

Allowed degree of service load, beyond which the component may not be regarded as applicable for reliably fulfilling its function by meeting the prescribed operating and maintenance conditions.

Function

Such objective to be reached that can be specified or defined without referring to the physical way for its achievement.

Functionality

The range or scope of those functions that may be performed by one system or equipment.

Credibility, validity analysis

Analysis performed during signal processing to filter the undoubtedly faulty data.

Pulse pipe

In general sense it is a data transmission channel to transfer the pressure (pressure difference) signals to the detector, including its all accessories (closing valves, cocks, filters, sedimentators, air traps, condense reference vessels, separation valves, attenuators etc). In narrow sense it is the pipeline constituting the signal transmission channel.

Device diversity

Redundant application of devices of different structure.

Reliability

The property of a system or device characterizing its ability to fulfill its intended function under the designed (considered) operating conditions for long time enough. Failure rate (relative number of losses of function/time), mean time to failure (MTTF) or in case of repairable (recoverable) components the mean time between failures can be used for characterization of reliability. Assuming that the statistical features of the failures follow Poisson-distribution, the time between failures or the failure rate are reciprocal to each other.

Self test, self verification

Self verification is that property of certain systems or components, by which they can make their function degradation or failure automatically detectable.

Passive safety equipment

Such equipment that is able to fully perform its safety function without auxiliary energy (e.g. bubble condenser tower, safety coolant tank).

Technological diversity

Redundant detection of the same events based on different process parameters.

Incorrect actuation of protection

Actuation of protection operation unjustified by the plant conditions.

Response time

The time difference between the occurrence of input value and output value; it is a characteristic value of dynamic features of a system. Its determination is made by the evaluation of response function to input signal shape (raise time, time constant etc.).

Expected lifetime

Statistical data characterizing the designable operating loads of the device. Depending on the type of operation of the device it can be expressed in terms of service life, load cycles etc. Its degree is strongly dependent on the actual operating conditions.

Protection operation

Actuation or operation of safety equipment, which is used for intervention in accident conditions and for mitigating the damages.

2.2. Definitions

ABOS	Safety classification of nuclear power plant components
NSC	Nuclear Safety Code

3. GENERAL DESIGN ASPECTS

This chapter formulates recommendation on complying with legal prescriptions in respect to general nuclear, and not just electric and I&C, safety related design requirements.

3.1. Selection principals of design aspects

The licensee, in order to meet the legal prescription, should determine or select the relevant and authoritative design requirements by reviewing the whole volume 3 of NSC.

This method for the determination of the requirements is justified, because some important requirements (life redundancy, reliability) are not only related to the electric and I&C systems, thus these are not included in the NSC chapters specific for the electric and I&C field (Chapter 5.3 of Volume 3 of NSC).

List of general design requirements recommended for consideration during the design tasks corresponding to electric and I&C systems and equipment is included in chapter 3.2 of this guideline.

Design requirements specific for the electric and I&C systems and components are discussed in chapter 4 of this guideline.

During the determination of relevant design requirements corresponding to the design task the licensee should consider the regulatory prescription, obligations included in the regulatory resolutions of legal force. In order to do that, prior to the commencement of the design task the licensee should inform the designer on the respective regulatory prescriptions and requirements.

During the determination of the recommendations related to design also the accepted international standards should be considered. During the design of electric and I&C systems and components fulfilling safety function also the recommendations of the International Atomic Energy Agency and the European Union should be considered. The most important ones are as follows:

a) IAEA No. NS-G-1.3.: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants,

b) IAEA No. NS-G-1.8.: Design of Emergency Power Systems for Nuclear Power Plants,

c) IAEA No. NS-G-1.2.:Safety Assessment and Verification for Nuclear Power Plants,

d) IAEA No. NS-G-1.1.: Software for Computer Based Systems Important to Safety in Nuclear Power Plants,

e) European Commission EUR 19265 EN: Common position of European nuclear regulators for licensing of safety critical software for nuclear reactors.

3.2. General recommendations on design

During the design tasks corresponding to electric and I&C systems and components the licensee should consider the following general design requirements interpretable also for electric and I&C systems and components. The text in italic contains the legal requirements; the normal text marks the recommendations for meeting the prescriptions.

"The safety systems, structures and components of the nuclear power plants shall be designed in a way that the nuclear power plant operation related nuclear safety objective, as well as the radiation protection and technical safety objectives supporting it shall be feasible." (NSC Volume 3, Section 2.001).

During the design task the achievement of the objectives specified in sections 2.003–2.004 of Volume 3 of NSC should be examined, the compliance should be justified.

„When designing a safety system, structure and component, the design schedule shall be prepared in a way that for the period of related licensing procedures all plans and certifications shall be available at the required phase in line with the regulations of licensing procedures". (NSC Volume 3, Section 3.001)

The design process should be determined by taking account of the licensing obligations.

"The safety functions and systems, structures and components fulfilling safety functions shall be classified based on their effect on safety". (NSC Volume 3, Section 3.004)

The safety classification should be performed. The definitions of the classes are included in 3.012-3.016 of Volume 3.

„During design, at first, the design specification of the safety systems, structures and components shall be determined." (NSC Volume 3, Section 3.005)

During the design the requirements should be determined for the systems or equipment, or for the different lifecycle phases of the new or modified system or equipment, and for the design process itself. The design specification should be elaborated by considering the applied prescriptions and standards, functional requirements, environmental and environmental resistance requirements, response time requirements, accuracy requirements, reliability requirements, testing requirements, modifiability demands, requirements on extendibility, limitations on accessibility, expectations on human-machine interface, and the requirements on performance, quality management and development process. The specification requirements should be determined and fixed in the initial phase of design, as appropriate. During the detailed design and implementation the compliance with requirements should be justified and certified.

"Throughout the whole lifetime of the nuclear power plant the compliance and allowability of interventions different from the approved conditions related to the safety classified systems, structures and components shall be justified by safety analysis." (NSC Volume 3, Section 3.039)

In case of modification of systems and components fulfilling safety function, or of their operating and other conditions, the allowability, and in this frame, the acceptability of the design specification should be justified by safety analysis. The effect of the establishment or modification on nuclear safety should basically be examined by deterministic analysis.

"The safety systems, structures and components shall be designed in a systematic way so that they could perform all required safety functions and with their assistance the anticipated operational occurrences, anticipated initiating events and to a reasonable extent the accident situations could be managed." (NSC Volume 3, Section 3.041)

Detailed design of the systems and equipment should be performed based on the specifications, and then the specified requirements should be justified and certified.

"The probabilistic safety analysis of the nuclear power plant systems shall be performed for the risk evaluation of the desired operation, and a judgment shall be made on its acceptability." (NSC Volume 3, Section 3.074.)

Based on the technical and operating conditions of the system or equipment fulfilling safety function the licensee should determine the effect of system or equipment failure or wrong actuation on core damage frequency, then the results should be evaluated for acceptability. If the design specification is available for the system or equipment, the acceptability should be examined based on conformity with the design specification.

"In order to achieve the required reliability of safety systems, structures and components the following design principles or a combination of them shall be applied:

a) redundancy,
b) diversity (functional, structural, operational, design, manufacture),
c) independence,
d) guaranteed quality in line with the requirements,
e) failure-proof design,
f) testability. (NSC Volume 3, Section 3.083)

The listed design principles should be applied during the design. Considerations for the application of design principles should be fixed in the design specification, the considerations on the applicability of the design principles should be justified by safety analysis.

"The availability of the safety function and the acceptable probability of its inadvertent operation from the aspect of the safety system is an external design requirement, which shall be satisfied by the individual reliability of the system's hardware and software components and by the resultant reliability appearing in the necessarily redundant and diverse architecture." (NSC Volume 3, Section 3.084.)

The availability of the safety function and the allowable probability of inadvertent actuation appear in the design specification of the system or equipment. During the detailed design end implementation the compliance with the requirements should be justified and certified.

"In the case of those redundant safety systems, structures and components where high reliability is required the system shall be protected against the common cause failures. In order to decrease the possibility of common cause failures the diversity and/or the independence principle shall be applied." (NSC Volume 3, Section 3.085)

During the design of safety related electric and I&C systems and components the design principles avoiding the common cause failures should be applied. The realization of protection against common cause

failures or the allowability of disregarding the requirement should be justified by safety analysis.

"The planned redundancy and independence of the safety system shall be sufficient to ensure that:

a) single failure does not cause the loss of the protection function,
b) the removal of any components or channels from operation does not result in the loss of the required minimum redundancy,
c) the natural phenomena, the external effects induced by human activities, effects of the normal operating condition and the design basis accidents do not result in the loss of the protection function." (NSC Volume 3, Section 3.087.)

The electric and I&C systems and components fulfilling safety function should be designed according to the requirements of the above a)–c) paragraphs. During the particular design tasks the acceptability of the considerations on the application of these requirements should be justified, and the applied requirements should be appeared in the design specification.

"To the possible extent the safety system, structure or component shall be designed in a way that its layout is transparent and simple and efforts shall be made to apply passive operational principles based on the laws of physics. The layout shall ensure the detection of failures in the safety systems at the time of occurrence, and with the help of the construction it shall provide for the possibility of simple elimination of the failures." (NSC Volume 3, Section 3.088.)

During the design of electric and I&C systems and components fulfilling safety function simplicity, appropriate failure detection capability and quick and simple reparability should be strived after.

"The safety system, structure and component shall be separated from all the other normal operational or safety functions. If this is not possible, then it shall be ensured that in the case of inoperability of any systems, structures or components performing different functions, the requirement for the safety function, the reliability, redundancy and independence related to the safety system shall be achieved, that is to say a connection like this shall not influence adversely the achievement of the safety function." (NSC Volume 3, Section 3.089.)

The systems and equipment fulfilling safety function should be designed and installed separated from the other safety classified and non-classified systems and equipment. If the criterion for separation cannot be complied

with, then a counter effect free connection should be established between the equipment.

"The design of the safety system, structure and component shall limit the probability of the operating personnel's intervention to the minimum decreasing the effectiveness of the safety system, structure or component. In places where reliable and quick protection operation are required such systems, structures and components shall be applied, which do not necessitate human intervention." (NSC Volume 3, Section 3.090.)

By increasing the automatism of the safety systems and equipment the possibility of human error, the probability of faulty interventions should be minimized. The requirements for automatism should be determined in the design specification; the acceptable level of automatism should be justified in safety analysis.

"The reliability of the safety system can not be verified solely by the theoretical considerations during the design phase, therefore during the manufacture, construction of the system and later in its lifecycle the testability shall be ensured, i.e. it shall be designed in a way that it could be removed from the operation and tested by inservice inspection. The operation of the safety functions shall be verified in its whole as the joint result of the system's required, resulting reliability adjusted to the interval of automatic or operator induced testing and technical evaluation." (NSC Volume 3, Section 3.091.)

Inservice testability of electric and I&C systems and components fulfilling safety function should be ensured. The requirements for testability should be determined in the design specification; the compliance with the requirements should be justified by safety analysis.

„Type testing shall be performed in order to demonstrate that the same type of equipment as those tested, to be used in the nuclear power plant will operate in line with the design requirements under the expected operating conditions. Functional testing of the components, modules, subsystems and where applicable the entire function, systems, system components shall be performed." (NSC Volume 3, Section 3.095.)

The compliance with the requirements determined in the design specification, the acceptability of the system or equipment should be justified by testing as well on the level of components and subsystems as of the entire system.

"The safety system, structure and component shall be arranged in a way that the number of unjustified operation shall be as low as possible." (NSC Volume 3, Section 3.096.)

Appropriate design solutions should be applied for minimizing the number of unjustified operation.

"The safety systems, structures and components, if required, shall be equipped with auxiliary systems. The redundancy, diversity, independence, reliability expectations of an auxiliary system, structure or component shall be in agreement with the requirements of the safety function, safety classification of the system, structure or component it is serving. In this respect the auxiliary systems (for instance coolant, power supply, lubricants, compressed air etc.) shall be considered as parts of the safety system, structure or component." (NSC Volume 3, Section 3.098.)

If the operation of a safety system requires auxiliary system, the design requirements for the auxiliary system should be determined based on the considerations to the requirements related to the safety system.

"During the design, manufacture, implementation and the control in production as well as the inspections of the systems, structures and components appropriately proven tools shall be effectively applied in line with the state-of-the-art knowledge and technology (for instance constructions, analysis methods, inspection tools). (NSC Volume 3, Section 4.002.)

During the design, establishment and different inspections of systems and equipment fulfilling safety function developed and adequately qualified procedures and tools should be used.

"The construction of the facility shall ensure that the sensitivity of the nuclear power plant for the possible failures is minimal. Following any postulated initiating event it shall be ensured, that

a) the safety systems comply with the single failure tolerance criterion, and the safety systems and components automatically actuated on real signal could not be hindered (for instance by false operator intervention),
b) following a failure or false intervention, due to the operation of the failure activated active protection, the nuclear power plant remains in a safe condition".." (NSC Volume 3, Section 4.003.)

The electric and I&C systems and components fulfilling safety function should be designed based on the above a)–b) requirements. During the

particular design tasks the considerations on the application of these requirements should be justified, and the requirements applied should be included in the design specification.

"The systems, structures and components shall be designed so that they entirely meet the high standard requirements while ensuring the following throughout the entire lifecycle of the nuclear power plant:
a) application of design requirements (standards),
b) material selection,
c) manufacture method,
d) possibilities of inspection and testing,
e) reparability,
f) maintainability,
g) replaceability." (NSC Volume 3, Section 4.004.)

The design of electric and I&C systems and components should be performed based on the relevant standards and fixed and justified design requirements.

If there is no appropriate requirement on the given design solution, then model experiment, reference or engineering judgment should be used to justify the acceptability of the applied design procedure or solution. (NSC Volume 3, Section 4.008.)

The adequacy of the applied technical solutions should be justified by referring to the respective design requirements or, if there is no such, by application references and description of the engineering judgment applied.

"The safety systems, structures and components performing operational function as well, shall be designed in a way that the execution of the safety function shall be of first priority against the operational function and the operational function should not prevent or endanger the execution of the safety function in any way. This condition shall be verified in the case of the involved systems, system components." (NSC Volume 3, Section 4.013.)

By appropriate design methods it should be ensured that the electric and I&C systems and components fulfilling safety and non safety functions the fulfillment of the safety function receives priority. Priority of fulfillment of safety functions should be justified by safety analysis and tests.

"Any connection between the safety system, structure and component and the connecting and adjacent systems, structures and component, which does not belong to the supply subsystems of the safety system, structure and component shall be eliminated. Temporary or permanent connection with

external system and component can only be achieved if the appropriate counter-effect protection separation is taken care of." (NSC Volume 3, Section 4.014.)

The systems and equipment fulfilling safety function should be separately designed and established from other safety and non safety classified systems and equipment. If the criterion on the separation cannot be met, then a connection protected against counter-effect should be established between the systems or equipment.

"Internal or external postulated initiating events and the failures induced by them shall not cause the operational failure of the safety system, structure and component which was designed to prevent the given operational incidents." (NSC Volume 3, Section 4.017.)

By the application of appropriate design solutions it should be ensured that the electric and I&C systems used for managing the postulated initiating events, and the consequential failures are protected against the effect of the incidents.

"The safety systems, structures and components shall be physically separated and they can not have common components or services." (NSC Volume 3, Section 4.018.)

The independence of systems and equipment fulfilling safety function of each other should be ensured.

„The safety systems, structures and components and their auxiliary systems shall be constructed so that they shall be protected to the most extent to the effects of internal and external sources of danger, including the interaction between the faulty safety systems, structures and components (for instance missiles, whipping of broken tubes, dynamic effects of discharging coolant, flooding) as well." (NSC Volume 3, Section 4.019.)

By appropriate design solutions it should be ensured that the electric and I&C systems and components and their auxiliary systems are protected against the effects of potential external and internal dangers.

„In accordance with the priority of the reliability requirements for each unit the regular inservice inspection, function testing of the safety systems, structures and components shall be ensured throughout the lifecycle of the nuclear power plant. The depth, interval, duration of the inspections and function tests shall be justified by analyses. If this is not applicable due to certain circumstances then further design solutions shall be applied or it

shall be justified that operation of appropriate duration can be sustained without the mentioned measures." (NSC Volume 3, Section 4.020.)

The condition of the systems and equipment fulfilling safety function should be inspected periodically; the features of the inspections – scope, method, frequency – should be determined and supported by safety analysis. The inspection requirements should be provided in the design specification.

"It shall be ensured that the operating personnel cannot intervene in the coast down of automatic protection operation and in the changing of the safe status during design basis accident until the protective activation conditions exist or at least for the time until the detailed directions are sufficient according to the analyses, and the protection algorithm is performed even if the signal activating the protective operation discontinues. The design shall ensure that the operating personnel could activate the protection operation, perform the required measures and have due information about the processes to be able to appropriately analyze the situation and perform all the required measures in their capacity." (NSC Volume 3, Section 4.021.)

Safety systems and equipment taking part in the handling of the design basis accidents should be designed by considering this requirement. The characteristics of their protection operation, the details of information for the personnel and the opportunities of the personnel to intervene should be determined and supported by safety analysis.

"The cycle period of function tests, the frequency of their revision, requirements for revisions, conditions and methods of maintenance in the case of safety systems, structures and components shall be identified during the design stage so that they are in agreement with the design principles, safety functions and classification of the safety systems, structures and components." (NSC Volume 3, Section 4.068.)

Characteristics of inspections related to electric and I&C systems and components fulfilling safety function should be specified by considering the applied design principles, technical features and the safety function to be fulfilled.

„The cycle periods of the safety systems and components function tests shall be justified by analyses. When performing the analyses the following functions shall be taken into account: the safety of the entire function's execution, the risks induced by the excessive load of the system, system component, as well as usage of the applied maintenance methodology, the

*classification, and the applied special design solutions (for instance redundancy, physical separation).” (NSC Volume 3, Section 4.*069.)

The adequacy of the testing requirements and procedures should be examined and supported by safety analysis. The analysis should be performed by considering the technical, operating and maintenance attributes of the system and equipment.

“The redundant systems, system components shall be physically separated. The separation shall be performed for their every single element (auxiliary systems, power supply etc.).” (NSC Volume 3, Section 4.094.)

During the design and construction of electric and I&C systems and components fulfilling safety function and having redundant structure the sets should be physically separated.

„The safety systems and components and auxiliary systems shall not form a common part of several nuclear power plant units unless it can be justified that such distribution cannot affect the total fulfillment of the safety functions including the situation when an anticipated operational occurrence or design basis accident occurs in one of the units or in planned shut down or when uploading is in progress.” (NSC Volume 3, Section 4.096.)

If an electric or I&C system or component fulfilling safety function is in connection with more nuclear power plant unit at the same time, then it should be justified that the system or the component is fully applicable to fulfill its safety functions and to meet the requirements of the design specifications even if accident conditions are assumed.

“In the cases of systems required to ensure the seismic protection of the nuclear power plant the single failure criterion shall be applied.” (NSC Volume 3, Section 4.108.)

The electric and I&C systems and components fulfilling seismic safety functions should comply with the single failure tolerance criterion.

“The nuclear power plant systems, system components shall be classified into seismic safety classes based on the safety function they perform during an earthquake.” (NSC Volume 3, Section 4.111.)

Based on the definition of the seismic safety classes the classification should be performed.

"In the case of structures and systems classified into the first and second seismic safety classes the load combinations of L1+SL-2 shall be taken into account at the design stage." (NSC Volume 3, Section 4.116.)

In the design of the system or equipment, or during the examination of compliance with seismic safety requirements the load combination of L1 + SL-2 should be considered in the seismic safety class 1 and 2.

„The safety systems, structures and components shall be protected by passive and active fire protection systems and shall be designed and implemented such a way that the probability and effects of fires and explosions induced by external or internal anticipated initiating events be as low as possible. The achievement of the safety objectives shall be ensured during and after the fire, irrespective of the operation of the active fire extinguisher systems." (NSC Volume 3, Section 4.124.)

In the design and establishment of electric and I&C systems and equipment fulfilling safety function appropriate fire protection systems should be applied considering that the fulfillment of the safety objectives should be ensured under and after the fire.

The fulfillment of design requirements specified in the law should be examined in every case irrespective of that the design task is to create a new equipment or system, or to modify an existing one.

The compliance with the design requirements should be described in detail in the design documentation of the electric or I&C system and component.

Recommendations on the single failure tolerance capability, the avoidance of common cause failures, redundancy, diversity, independence, failure management and testability are also addressed in Guideline 3.12 („Specific guidance on the design of nuclear power plant components"). These recommendations are also considered in the design task.

3.3. Application of standards

Based on the laws effective on the day of issuance of this guideline (Act XXVIII of 1995 and Act CXII of 2001) the application of standards is voluntary, however irrespective of that the design tasks should be performed by considering the standards.

The standards that could be used in design should be specified and recorded in the design specification. The acceptability of the designated scope and the

compliance with the content of the standards should be justified during the design task and the implementation.

The design is performed by as wide as possible application of the domestic, the IEC- and the ISO- standards.

Listing of the most important standards belonging to the design of electric and I&C systems and components fulfilling safety function are included in the Sections 4.1.2, 4.2.2 and 4.3.2 of this guideline. The lists are not full lists.

4. SPECIFIC DESIGN ASPECTS

The special design requirements on the electric and I&C systems and components fulfilling safety function are discussed in chapter 5.3 of Volume 3 of the Nuclear Safety Code but, in addition, the chapter 5.1 containing the design requirements on the reactor and the active core also formulates requirements for the I&C systems fulfilling reactivity control and reactor protection safety functions.

Below, the guideline describes the special design requirements related to the systems and equipment by formulating recommendations for the fulfillment of the requirements. The recommendations are discussed in three chapters in the following grouping:

a) electric power supply systems and electric equipment,

b) instrumentation and control systems and equipment,

c) specialties of programmable systems and equipment.

The guideline discusses the special design requirements relevant for both electric and I&C field both in chapter 4.1 and 4.2. Recommendations on systems and equipment of measurement techniques are included in chapter 4.2.

During the design tasks the licensee should perform the choice of the relevant design requirements by reviewing the subchapter, as appropriate. The relevant requirements and recommendations for the design tasks of electric power supply are included in chapter 4.1 of the guideline. As far as the design of the measurement and I&C systems are concerned the chapter 4.1 and 4.2 includes recommendations. If the electric power supply system or the I&C system contains programmable equipment, for the determination of the specific design requirements the licensee should consider the chapter 4.3 also.

In the sections 4.1.1, 4.2.1 and 4.3.1 the text in italic means legal requirement, while the normal text marks the recommendation related to the fulfillment of requirement.

4.1. Electric power supply systems and electric equipment

4.1.1. Recommendations on design

"Every disturbance – information deteriorating circumstance – shall be analyzed during the signal transmission and measures shall be introduced to decrease the disturbance as much as possible. The separation and counter effect free condition and justification of I&C systems shall be ensured." (NSC Volume 3, Section 5.057.)

The requirements basically addresses I&C systems, but also the electric power supply systems and equipment should be provided with appropriate disturbance protection. Beside the development of disturbance protection the noise signals superposed on the supply voltage in the electric power supply systems should be filtered or minimized by filtration. The design requirements on disturbance protection should be included in the design specification.

"At the design stage those general requirements shall be taken into account which the systems and components shall satisfy throughout their entire lifecycle. The components of the system shall comply with the functional, reliability, performance, environmental resistance requirements throughout their entire lifecycle." (NSC Volume 3, Section 5.062.)

The detailed design should be performed based on the design specification. The determination of the design requirements (specification) should be based on the lifetime, operating conditions, functionality, reliability, performance and environmental resistance expectations. The adequacy of design requirements should be justified by safety analysis.

"The power supply of the safety I&C engineering systems shall originate from such source, the reliability of which is in agreement with the importance of the safety function and task of the I&C system." (NSC Volume 3, Section 5.067.)

The electric power supply of I&C systems fulfilling safety function should be designed by taking account of the availability and reliability requirements of the system fulfilling safety function. The acceptability of

technical solutions, the compliance with the requirements, should be justified by safety analysis.

"Appropriate electric power supply system shall be designed for the operation of the nuclear power plant, which ensures the operation of the safety systems and components, under all operating conditions of the design basis." (NSC Volume 3, Section 5.071.)

The electric power supply systems are designed to fully meet the consumer demands determined by the specifications. The design of electric power supply systems and equipment fulfilling safety functions should be performed by considering every possible state of the design basis including normal operation and accident situations and their consequences. As appropriate, the operability of systems fulfilling safety function should be ensured in accident situation as well. The adequacy of design considerations and technical solutions should be justified by safety analysis; the respective requirements should be included in the design specifications.

"The design shall be conducted in compliance with the requirements of such acknowledged regulations, guidelines and standards, which are applicable to provide the functionality required by functions, systems and system components classified into safety classes, at a high standard." (NSC Volume 3, Section 5.072.)

The design task should be performed by considering the respective legal prescription, related design aids (recommendations), the valid rules and the proven technical solutions with due reference.

"A supply method shall be the part of the electric power supply system which, in design basis accident situation, when the off-site electric power supply is entirely inaccessible, automatically ensures electric power supply to the systems and system components required for the safe shut down of the reactor and to remove the residual heat. This system shall be independent of the national electric power network, of the normal electric power supply system of the nuclear power plant, and the operability and operation of which can be ensured for the long term." (NSC Volume 3, Section 5.073.)

The electric power supply system should be constructed such a way that could, in case of disturbance of the national electric power network, ensure the electric power with due quality and reliability for the shut down and cooling down of the reactor and keeping it in a safe cold state, as well as for the management of design basis accidents. The adequacy of design

considerations and technical solutions should be justified by safety analysis; the respective requirements should be included in the design specification.

"The load of electric power supply systems and system components, in none of the operating states of the design basis, may exceed the limit values defined in the design specifications." (NSC Volume 3, Section 5.074.)

Both in normal and in design basis accident situations the permissible nominal loads of the electric power supply systems and their components fulfilling safety function should be limited by considering their capabilities. Recommendation on limiting the loads should also be considered for the normal service power supply systems, as appropriate. Requirements on the electric load limitations of systems and equipment should be included in the design specifications, and the acceptability should be justified by safety analysis.

"The operational events occurring in the normal electric power supply system of nuclear facilities shall not affect the nuclear safety of the facility." (NSC Volume 3, Section 5.075.)

By the application of appropriate design solutions the protection of systems and equipment fulfilling safety function should be ensured against the operating disturbances of normal operation and other safety system and against the effect of accidental events. The electric power supply of systems and equipment fulfilling safety function should be constructed on the base of safety electric power supply systems. The adequacy of design considerations and technical solutions should be justified by safety analysis; the respective requirements should be included in the design specifications.

"The physical separation of redundant safety electric power supply systems and the normal and safety electric power supply systems shall be achieved. In cases where the physical separation of the safety electric power supply systems and the normal electric power supply systems is not feasible other tools shall be ensured and the counter effect free condition shall be provided and justified." (NSC Volume 3, Section 5.076.)

The safety electric power supply systems of redundant structure should be designed with physical separation. The physical separation should be considered for the construction of the connection of the normal and safety electric power supply systems. If the physical separation cannot be realized then counter effect free connection should be designed. Design considerations on the separation of systems and on the counter effect free

connection should be justified by safety analysis; the respective requirements should be included in the design specifications.

"In technological spaces only those safety cables can be lead through, which connect to the technological system components located there. These cables shall have separation in order to protect them from the dangers induced by the failure of the system component. The separation of cables connected to redundant systems, system components shall ensure that the dangers induced by the failure of one of the systems, system components do not affect the cables of the other safety system, system component."(NSC Volume 3, Section 5.077.)

By the application of appropriate design solutions the protection of the cables fulfilling safety functions should be ensured against every possible external damaging effect. The adequacy of the design considerations and technical solutions related to cabling should be justified in safety analysis and the respective requirements should be included in the design specifications.

In the technological spaces only the cables of the technological system components located there should be placed.

"If in the technological rooms cable leading through is unavoidable then the safety cables shall have separation and protection which ensures that their operability in every operating condition of the design basis exist to a sufficient extent to execute their tasks." (NSC Volume 3, Section 5.078.)

The recommendation formulated for requirement 5.077 is also relevant for this one. By the application of appropriate design solutions the protection of the cables fulfilling safety functions should be ensured against every possible external damaging effect. The recommendation is of general validity; it covers all normal operating and accident conditions, and is independent of the cable routes.

"Coupled electric connections can be implemented only if they exclude the inadvertent loss of function induced by the breaking of the circuit." (NSC Volume 3, Section 5.079.)

In the design of coupled electric connections such technical solutions should be applied that can prevent the inadvertent breaking of the circuits. The requirements related to electric connections should be included in the design specifications.

"The electric intervention instruments shall be supplied from a reliable network of appropriate availability. The design of the energy supply system shall ensure the protection against unallowable electric power load with sufficient selectivity and efficiency." (NSC Volume 3, Section 5.085.)

The electric power supply of electric intervention instruments should be designed by considering the specification of the intervention instrument, on operability and availability of the instrument and on the requirements of its other technical parameters and data.

Appropriate technical solutions should be applied for the design of the electric power supply systems to manage the electric incidents and events, and to detach the failed electric equipment or part networks. The adequacy of design requirements and technical solutions should be justified in safety analysis and the respective requirements should be included in the design specifications.

"Closed (plugged, socket) connections in the main and the control electric circles of the executive instruments may only be applied if the connected condition is directly or in a direct way detectable. Direct check shall have priority". (NSC Volume 3, Section 5.086.)

Detachable electric connections should be applied during the design only if the adequacy of the connections may be continuously and unambiguously checked. The requirements related to electric connections should be included in the design specifications.

"The power supply systems, system components shall be grouped, beyond the safety classification, according to the permissible loss of electric power supply. The design of the electric supply network of the nuclear power plant shall be based on this." (NSC Volume 3, Section 5.087.)

The electric power supply systems and equipment should be categorized based on the permissible loss of electric power supply. The categorization should be made according to the following definitions.

Category I: uninterrupted electric power supply systems

Those electric systems and equipment belong to this category, which are necessary for the electric power supply of equipment required for the safe shutdown and cooling of the reactor.

Category II: Vital power supply systems

Those electric systems and equipment belong to this category, which are necessary for the safe shutdown and cooling of the reactor.

Category III: systems providing backup and normal service electric power supply.

Backup electric power supply is necessary for the uninterrupted power supply of non-safety systems. Those electric systems and equipment belong to this category, which are in direct connection with the shutdown and cooling of the reactor, or are important from any aspect of the operation, or the loss of electric power supply could lead to the failure or loss of function of equipment of high value. Normal service electric power supply is ensured for those electric systems and equipment, for which there is no time constraint prescribed for the loss of supply of the supplied consumers or the supplied equipment has no relevance in the shutdown or cooling of the reactor.

The category of the electric power supply systems determined above should be included in the design specification.

"The loss of uninterrupted power supply can be 3 seconds at the most; the loss of vital power supply can be 1 minute at the most." (NSC Volume 3, Section 5.088.)

Design limitations corresponding to the loss of electric power supply should be considered during the design tasks. Compliance with the limitations should be justified.

"Appropriate quantity of independent supply shall be ensured to operate the systems, system components classified into safety classes." (NSC Volume 3, Section 5.089.)

The design of the safety electric power supply systems should be performed by considering the consumer demands and the general and specific design requirements for the safety systems.

"The safety electric supply systems shall be equipped with automatic switching technology which, in case of operational supply loss or when the parameters go above or under the required value limits, automatically switches over to backup supply."(NSC Volume 3, Section 5.090.)

By the application of appropriate design solutions and backup supplies the electric power supply of the systems and equipment fulfilling safety function should be ensured for the case of failure of the normal operating supply (assuming maximum power demand). Design considerations and technical solutions related to the electric power supply should be justified in

safety analysis and the respective requirements should be included in the design specifications.

"The uninterrupted, vital energy supply of system components of the safety systems in nuclear facilities shall be ensured from backup power source beside the independent electric power supply. The backup power sources shall have the capacity to be capable of independently supplying the electric instruments in design basis accident situations." (NSC Volume 3, Section 5.091.)

By the application of appropriate design solutions and backup supplies the electric power supply of the systems and equipment fulfilling safety function should be ensured for the case of failure of the normal operating supply (assuming maximum power demand). Design considerations and technical solutions related to the electric power supply should be justified in safety analysis and the respective requirements should be included in the design specifications.

"Continuous, uninterrupted electric power supply shall be available for the reactor control room systems, system components, where necessary." (NSC Volume 3, Section 5.094.)

If based on the safety analysis the fulfillment of the safety function is continuously necessary, the requirement on the continuousness should be taken into account in the design and construction of the system or equipment fulfilling the function. The adequacy of the design considerations and technical solutions should be justified in the safety analysis; the requirements should be included in the design specification of the concerned systems or equipment.

4.1.2. Application of standards

The most important standards addressing the design of electric power supply systems and equipment fulfilling safety function are as follows:

a) MSZ 171-1:1984: Common safety requirements of electric products
b) MSZ 172-1:1986: Contact protection rules. Low voltage high current electric equipment
c) MSZ 2364-100:1995: Establishment of electric equipment of at most 1000 V voltage and high current
d) MSZ EN 50178:1998: Electric equipment that can be used in high current facilities

e) MSZ EN 61660-1:1999: Short circuit currents in the direct-current auxiliary equipment of power stations and substations. Part 1: Calculation of short circuit currents (IEC 61660-1:1997)

f) MSZ EN 61660-2:1999: Short circuit currents in the direct-current auxiliary equipment of power stations and substations. Part 2: Impact calculations (IEC 61660-2:1997)

g) MSZ IEC 50(448):1997: International electric engineering dictionary. Volume 448: Protection of electric power systems

h) MSZ 172-3:1973: Contact protection rules. Equipment of at most 1000 V voltage, directly grounded

i) MSZ 172-4:1978: Contact protection rules. Equipment of at most 1000 V voltage, low short circuit current

j) MSZ EN 60529:2001: Protection grades ensured by covers of electric products (IEC 529:1989)

k) MSZ EN 45510-2-8:2004: Guidelines on acquiring power plant equipment. Part 2-8: Electric equipment. Cables of high voltage

l) IEC 60780: Qualification of electrical items of the safety system for nuclear power generating stations

4.2. Instrumentation and control systems and equipment

4.2.1. Recommendations on design

"The reactor protection shall be diverse regarding the detection of the postulated initiating events and the activation of the protective operation. In the case of postulated initiating events causing the reactor protection operation the activation of the protection shall be initiated by two different physical characteristic, individually having the required redundancy, exceeding the value limits (pressure, power, temperature etc.), so that any of the two could initiate the reactor protection operation alone and it shall not result in a consequence substantially different from the consequence defined for the given operational incident. (NSC Volume 3, Section 5.016.)

The I&C system realizing the so-called reactor protection function should be designed by considering the design principles for redundancy and diversity. The diversity should be implemented both for detection and activation of protection. The adequacy of design principles and technical solutions applied should be justified in safety analysis and the design requirements should be included in the design specifications.

"It shall be ensured that the activated reactor protection, together with the operation of the systems and system components automatically activated by the reactor protection could not be interrupted. (NSC Volume 3, Section 5.017.)

The priority of the coast down of the reactor protection operation should be ensured by the application of appropriate design solutions over the operator and other automatic interventions. Design considerations and technical solutions on the coast down of the reactor protection operation and the priority of the operation should be justified by safety analysis, the respective requirements should be included in the design specifications.

"At least one of the two reactivity regulating and safety systems shall be capable of bringing the reactor into subcriticality of sufficient safety margin from every operating condition of the design basis in a sufficiently short period of time (a couple of seconds), and of keeping it there for the required period of time. In meeting the requirement the advertent activities such as increasing reactivity in shut down condition (for instance moving the absorbent because of maintenance, refueling activities) shall be taken into account, as well as the single failure occurring in the reactivity regulating and safety systems and system components." (NSC Volume 3, Section 5.018.)

It should be ensured by the application of appropriate design solutions that the I&C systems fulfilling so-called reactor protection and reactivity regulation functions are applicable in every operating state and accident conditions to safely shut down the reactor and permanently keep it there by assuming single failure. During the design the activities performed on the shut down reactor entailing reactivity change should be considered. The adequacy of the design considerations and technical solutions should be justified in safety analysis, and the respective requirements should be included in the design specifications.

"The design of the reactivity regulating and the safety protection systems shall prevent that the fuel element design value limit is exceeded even in the case of single failure." (NSC Volume 3, Section 5.019.)

It should be ensured by the application of appropriate design solutions that the I&C systems fulfilling so-called reactor protection and reactivity regulation functions can provide the prevention of exceeding the design value limit of the fuel element even if single failure is assumed. The adequacy of the design considerations and technical solutions should be

justified by safety analysis, and the respective requirements should be included in the design specifications.

"The design of the reactivity regulating and the safety systems shall ensure that in every operating state of the design basis exceeding the temperature limit of the fuel and the cooling system as well as the limits of other related safety parameters is excluded." (NSC Volume 3, Section 5.02.)

The safety I&C systems fulfilling reactor protection and reactivity regulating functions should be designed such a way that the operation of the systems excludes the exceeding of the safety limiting parameters related to the fuel and the reactor coolant system. These criteria should be met for each normal operating and accident state involved in the design basis. The adequacy of the technical solutions and compliance with the design requirements should be justified by safety analysis; and the respective requirements should be included in the design specifications of the safety systems.

The design of the reactivity regulating and the safety protection systems shall ensure that even their unanticipated operation does not cause the exceeding of the extent and rate of reactivity change limits. (NSC Volume 3, Section 5.021.)

By the application of appropriate design solutions it should be ensured that the failure of safety I&C system fulfilling reactor protection and reactivity control function does not cause the impair of the design limits of reactivity change. The adequacy of the technical solutions and compliance with the criteria should be justified by safety analysis; and the design criteria should be included in the design specifications of the safety systems.

"The design of both reactivity regulating and safety systems shall be designed such a way that ensure that the safety function of the system could be performed in case of single failure, with the help of any of the on-site or off-site electric power supply, even if it is assumed that the worthiest control rod is stuck." (NSC Volume 3, Section 5.022.)

The design of the safety I&C system fulfilling reactor protection and reactivity control function should be performed by considering the single failure criteria and making a further assumption on the stuck of the worthiest control rod. The adequacy of the systems to fulfill the function should be justified by safety analysis; and the design criteria should be included in the design specifications of the systems.

The application of some of the reactivity regulating and protection systems and system components is permitted to regulate the power of the core in normal operation, if the capability to shut down the reactor is permanently available. (NSC Volume 3, Section 5.023.)

If the regulation of the reactor in normal operation is realized through safety I&C systems fulfilling reactor protection and reactivity regulating functions, then the protection task should have priority. Compliance with the design criteria and the applied technical solutions should be justified by safety analysis; the design criteria should be included in the specification of the systems.

"Control and measurement instruments shall be applied to control the parameters of the safety systems and components during normal operation and anticipated operational occurrences and design basis accidents. Special attention shall be paid to those operational parameters and systems, system components, which may influence the fission process, the cooling of the core, the removal of the residual heat, the integrity of the fuel element, the primary circle and the containment, and those information, which are required for the safe, reliable operation of the nuclear power plant." (NSC Volume 3, Section 5.053.)

In all operating and accident situations the monitoring of the parameters of I&C systems fulfilling safety function, especially of safety systems fulfilling basic safety functions, should be ensured by the application of appropriate design solutions. Compliance with the design requirement and the adequacy of the corresponding technical solutions should be justified by safety analysis. The requirement should be included in the design specification of the systems.

"Every anticipated failure, which significantly diverts one or more parameters of the nuclear power plant from the safe values, shall be identified and evaluated in order to prevent the failure or to eliminate its effects." (NSC Volume 3, Section 5.054.)

The failure possibilities of systems and equipment, and the potential consequences should be examined during the design. If, as a consequence of failure, the technological or nuclear parameters of the nuclear power plant may depart from the safe operating range, then appropriate design solutions should be applied to prevent the failure or to manage it safely. Compliance with the design requirement and the technical solutions performing that should be justified by safety analysis. The requirement should be included in the design specification.

"The instrumentation and control engineering configuration of the safety systems, system components, and the signal interface between the system component and the technology required to detect the occurrence of events shall be in direct, known and unambiguous connection with the behavior, physical parameters of the reactor unit." (NSC Volume 3, Section 5.055.)

The structure, functionality and other features of the I&C systems fulfilling safety function should be designed based on the corresponding technological systems, and the characteristic physical processes and physical laws. Compliance with the requirements should be justified by safety analysis. The design requirements should be included in the design specification of the systems.

„In cases when the measurement of a physical parameter is not feasible to detect an event in practice, then the deducted parameter considered instead shall be in known and tight physical and time connection with the event to be detected." (NSC Volume 3, Section 5.056.)

If the detection of an event is based on a derived parameter of the I&C system fulfilling safety function, then such signal should be applied as a parameter supporting its operation, which is in unambiguous and well defined relation to the detected event. Compliance with the requirement should be justified by safety analysis. The requirement should be included in the design specification of the systems.

"Every disturbance, every circumstances deteriorating the information shall be analyzed during the signal transmission and measures shall be introduced to decrease the disturbance as much as possible. The separation and counter effect free condition of the safety and revision control engineering systems shall be ensured." (NSC Volume 3, Section 5.057.)

In order to ensure the disturbance protection and minimization of disturbance sensitivity of the signal and data transmission channels appropriate design solutions should be applied. The requirements related to disturbance protection and disturbance sensitivity should be included in the design specifications.

The systems and equipment fulfilling safety function should be designed separated from other systems fulfilling safety and operating functions. If the separation is not possible, then counter effect free connection should be developed. The requirements for the separation of the system, the properties of signal and data connections should be included in the design

specifications. The requirements and the applied technical solutions should be justified by safety analysis.

„All possibilities should be excluded to change the instrumentation and control engineering configuration, operating logic, or the connecting data of the safety system, system component, by occasional or readily available maintenance or test solutions, which are not designed for that function or are not under strict administrative control." (NSC Volume 3, Section 5.058.)

Modification of properties of the systems and equipment fulfilling safety function should be carried out in an intentional and supervised way, by application of tools and procedures developed for the implementation of the modification. Appropriate design and technical solutions should be applied to prevent the inadvertent and not adequately supervised modifications. Compliance with the design requirements and the applied technical solutions should be justified by safety analysis. The requirements for the modification should be included in the design specification.

„Control and measurement instrumentation shall be implemented in order to monitor the occurrence of radioactive materials and to measure their quantity at every such locations where their release to the environment is possible." (NSC Volume 3, Section 5.059.)

Appropriate instrumentation should be developed and applied for monitoring and measurement of environmental release of radioactive materials. The design considerations on development, installation and selection of instrumentation should be justified by safety analysis.

"The implementation and application of instrumentation and control engineering systems shall ensure the measurement of safety relevant operational parameters of the nuclear power plant that indicate the conditions of the nuclear power plant, the automatic registration and archiving possibility of the instructions given to the components and of the measurement results, thus enabling the tracking and later analysis of operating conditions of the design basis." (NSC Volume 3, Section 5.060.)

The nuclear power plant instrumentation and control systems should be developed to enable, in the relevant scope, the automatic measurement of operational and safety relevant parameters characterizing the state of the plant and the registration and archiving of measured values and activating signals with due resolution. The adequacy of design considerations and compliance with the requirements should be justified by safety analysis.

'The measurement domain shall cover the entire range of the measured parameter, including the characteristic value range of normal and design basis accident operating conditions. Measuring circuits of overlapping measuring limits shall be applied, if necessary." (NSC Volume 3, Section 5.061.)

The measuring limit of measuring circuits should be determined by taking account of the extreme values of the parameters to be measured and of the necessary resolution. The requirements for the determination of the measurement range and the measuring circuit should be included in the design specifications. The requirements and the applied technical solutions should be justified by safety analysis.

"In the design stage those general requirements shall be taken into account which the systems, system components shall satisfy throughout their entire operational lifetime. The components of the system shall comply with the functional, reliability, performance, environment resistance requirements throughout their entire lifetime." (NSC Volume 3, Section 5.062.)

The detailed designs should be performed based on the design specification. The determination of the design requirements (specification) should be determined by considering the expectations on the lifetime, operating features, functionality, reliability, performance, environmental resistance. The design requirements should be justified by safety analysis.

"A part of the control and measurement instruments shall be capable of providing information on the conditions of the nuclear power plant during and after accidents for the emergency response decision-makers." (NSC Volume 3, Section 5.064.)

Appropriate supporting instrumentation should be designed and established for the emergency response decision-making. The design considerations and technical solutions should be justified by safety analysis.

"The signals related to the protection shall not be self confirming, irrespective of the existence of the postulated initiating event. The signals related to the protection shall be confirmable by the intervention of the personnel even if the value limits are not exceeded any longer." (NSC Volume 3, Section 5.066.)

By the application of appropriate design solutions it should be ensured that the confirmation of the control room signals related to protection operation is possible only by operator intervention. Erasing of control room signals subsequent to the confirmation should only be possible after elimination of

the deviation causing the protection operation. Compliance with the requirements related to the confirmation and erase of signals should be justified. The requirements should be included in the design specifications.

"The minimum configuration of the safety related instrumentation, by which the operation of the reactor unit is acceptable and the acceptability shall be justified." (NSC Volume 3, Section 5.068.)

In the design of the nuclear power plant unit that minimum configuration of instrumentation should be determined by the availability of which the operation of the unit is acceptable from nuclear safety point of view The designated minimum configuration should be justified by safety analysis.

"The safety control and measurement instruments shall be designed to make the detection of the failure of the equipment or the exceeding of measuring range of a given quantity is possible by appropriate signals or by any other reliable way." (NSC Volume 3, Section 5.069.)

The measurement circuits fulfilling safety function should be designed to be able to detect the failure of the instruments or circuits. Compliance with the design requirement and the applied technical solutions should be justified by safety analysis. The requirement on failure detection should be included in the design specification of the measuring circuit of the instrumentation and control system.

Exceeding of the measurement limit of the quantity to be measured is not allowed based on the general design requirements; its occurrence is design failure.

„The design shall be conducted according to the requirements of acknowledged regulations, guidelines and standards, which are applicable to provide the functionality required by functions, systems, system components classified into safety classes, at a high standard." (NSC Volume 3, Section 5.072.)

The design task should be performed according to the respective legal prescriptions, relevant design aids (recommendations), effective standards and proven technical solutions with due reference.

"In technological spaces only those safety cables can be lead through, which connect to the technological system components located there. These cables shall be separated in order to protect them from the dangers induced by the failure of the system component. The separation of cables connected to redundant systems, system components shall ensure that the dangers

induced by the failure of one of the systems, system components do not affect the cables of other safety systems, system components.“ (NSC Volume 3, Section 5.077.)

The protection of the cables fulfilling safety functions should be ensured against every possible damaging effect by the application of appropriate design solutions. The cables of safety systems should be lead in individual routes protected from or independent of other systems. The adequacy of design considerations and technical solutions of the cables should be justified by safety analysis and the respective requirements should be included in the design specifications.

In technological spaces only those safety cables can be located and lead through, which connect to the technological system components operated there.

“If in the technological rooms the cable lead through is unavoidable then the safety cables shall have separation and protection, which ensures that their operability in every operating condition of the design basis exist to a sufficient extent to fulfill their functions.” (NSC Volume 3, Section 5.078.)

The recommendation provided to paragraph 5.077 is also relevant to this requirement. The protection of cables fulfilling safety function should be ensured by the application of appropriate design solutions against every possible external damaging effect. The recommendation is of general sense; it covers all operating and accident states, and independent of the cable routes.

“Coupled electric connections can be implemented only if they exclude the inadvertent loss of function induced by the breaking of the circuit.” (NSC Volume 3, Section 5.079.)

In the design of coupled electric connections such technical solutions should be applied that can prevent the inadvertent breaking of the circuits. The requirements related to electric connections should be included in the design specifications.

“In the case of each safety operation signal shall be provided for the operating personnel, which informs them on that the violation of which criterion induced the activation. Reliable notification shall be provided to the operating personnel on the real execution of the safety interventions. This notification shall come from a primary process variable, but if it cannot be provided then the position signal of intervention tools shall be

sufficiently reliable. Possibility shall be provided to activate the safety operation manually." (NSC Volume 3, Section 5.080.)

At those protection operation, the activation of which may be induced by more events (e.g. scram), the event activated the operation shall be identified (control room signal). Beside the identification of the initiating event information should be provided to the operating personnel on the characteristics of coast down of the protection operation and on the conditions of the implementation of the protection intervention. The instrumentation and control system should be designed to ensure the manual initiation of the protection operation.

Design considerations and applied technical solutions related to the development of launching of protection operation and coast down, and the control room signals should be justified by safety analysis. The design requirements should be included in the design specifications of the systems.

„The intervention instruments shall comply with the requirements of the valve to be driven and the technology in the environmental conditions of all operating conditions of the design basis." (NSC Volume 3, Section 5.081.)

The design of the valve drive mechanisms should be performed by considering the technical and operating conditions of the valve, and the environmental parameters characteristic of the design basis accident, loads.

The adequacy of design considerations and applied technical solutions should be justified by safety analysis. The design requirements should be included in the design specification of the operation circuit.

"In the selection of the intervening instrument those excess loads shall also to be taken into account, which may be induced by the rigidity of the mechanical torque transmission or by the failure of the torque switch. The valve and the intervening instrument shall be designed to tolerate the excess loads." (NSC Volume 3, Section 5.082.)

The requirement can be interpreted as part of paragraph 5.081. The design of the valve drive mechanisms should take into account the excess loads originating from the rigidity of the mechanical torque transmission or from the failure of the torque switch. The adequacy of the related designer considerations and applied technical solutions should be justified by safety analysis. The design requirements should be included in the design specification of the operating circuit.

The relays controlling the operation of the intervention instrument, its limits and boundaries shall be reliable enough by themselves to ensure that their potential failures do not limit the availability of the executing instrument. The limit switches of the executing instrument shall be generally independent of the similar elements of the driven valve. If this can not be ensured then the mechanical limit switch of the executive instrument shall be in an unambiguous and reliable mechanical connection with the status of the intervention instrument. (NSC Volume 3, Section 5.083.)

The design of the valve drive mechanism should consider the requirements for availability and reliability of the executing instrument. The adequacy of the design considerations and the applied technical solutions should be justified in safety analysis. The design requirements should be included in the design specifications.

"The torque switches and their operational algorithm shall be designed to ensure that their on and over switch torque transients do not induce the shut down of the intervention instrument." (NSC Volume 3, Section 5.084.)

The design of the valve drive mechanisms should consider the requirements for the torque switches. Compliance with the requirements should be justified in safety analysis.

"Closed (plugged, socket) connections in the main and control electric circuits of the executing instruments may only be applied if the connected condition directly or in a direct way is detectable. Direct verification shall have priority." (NSC Volume 3, Section 5.086.)

In the design detachable electric connections are applied for electric safety reasons. The acceptability of the connections should be unambiguously verified after regular maintenance during each outage by full scope function test or, in case of occasional maintenance, by a test commensurate with the intervention. The requirements for electric connections should be included in the design specifications.

"The displays of process variables functionally connected to one another and the status displays of the controls of these process variables shall be, in order to be easily and reliably managed, arranged in groups based on the ergonomic requirements. The signals providing the information shall produce appropriate visual and sound signals." (NSC Volume 3, Section 5.096.)

Instrumentation of control rooms should be designed by considering the functional and ergonomic requirements. The adequacy of design

considerations and technical solutions should be justified by safety analysis; the respective requirements should be included in the design specifications.

4.2.2. Application of standards

The most important specific standards related to the design of the I&C systems and equipment fulfilling safety functions.

a) MSZ EN 61508-1:2002 Operational safety of electric/electronic/programmable safety systems. Part 1: General requirements (IEC 61508-1: 1998+1999 amendments)

b) MSZ EN 61508-2:2002 Operational safety of electric/electronic/programmable safety systems. Part 2: Requirements for electric/electronic/programmable safety systems (IEC 61508-2:2000)

c) MSZ EN 61508-3:2002 Operational safety of electric/electronic/programmable safety systems. Part 3: Software requirements (IEC 61508-3:1998+1999 amendments)

d) MSZ EN 61508-4:2002 Operational safety of electric/electronic/programmable safety systems. Part 4: Definitions and abbreviations (IEC 61508-4:1998+1999 amendments)

e) MSZ EN 61508-5:2002 Operational safety of electric/electronic/programmable safety systems. Part 5: Examples for determinations of safety integrity levels (IEC 61508-5:1998+1999. amendments)

f) MSZ EN 61508-6:2002 Operational safety of electric/electronic/programmable safety systems. Part 6: Guidelines for application of the IEC 61508-2 and the IEC 61508- (IEC 61508-6:2000)

g) MSZ EN 61508-7:2002 Operational safety of electric/electronic/programmable safety systems. Part 7: Review of techniques and measurements (IEC 61508-7:2000)

h) MSZ EN 61511-1:2005 Operational safety. Safety systems of industrial process control. Part 1: Framework system, definitions, requirements for the system, hardware and software (IEC 61511-1:2003 + 2004 amendments)

i) MSZ EN 61511-2:2005 Operational safety. Safety systems of industrial process control. Part 2: Guidelines for application of IEC 61511-1 (IEC 61511-2:2003

j) MSZ EN 61511-3:2005 Operational safety. Safety systems of industrial process control. Part 3: Guidelines for the determination of required safety integrity levels (IEC 61511-3:2003 + 2004 amendments)

k) IEC 6068: Environmental testing, Basic environmental testing procedures

l) IEC 60231: General principles of nuclear reactor instrumentation

m) IEC 60231D: Principles of instrumentation for pressurized water reactors

n) IEC 60639: Nuclear reactor. Use of the protection system for non-safety purposes.

o) IEC 60671: Periodic tests and monitoring of the protection system of nuclear reactors

p) IEC 60709: Separation within the reactor protection system

q) IEC 60801-1.,2.,3.,4.: Electromagnetic compatibility for industrial-process measurement and control equipment

r) IEC 60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

s) IEC 60980: Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations

t) IEC 601025: Fault tree analysis (FTA)

u) IEC 61508: Functional Safety: safety-related systems.

v) IEC 61513: Nuclear Power Plants. Instrumentation and control for systems important to safety. General requirements for systems.

4.3. Specialties of programmable systems and equipment

4.3.1. Recommendations on design

„In the design stage of computer based systems, system components in accordance with the present regulation all the valid, applicable standards shall be taken into consideration." (NSC Volume 3, Section 5.099.)

The design of the programmable systems and equipment fulfilling safety function should be performed by considering the legal requirements, relevant standards and laws. The scope of standards to be applied should be included in the design specification.

"In the case of computer based systems classified into ABOS 2 safety class the following system characteristics shall be realized and justified:

a) The computer based system is of deterministic operation.

b) The programme performing the safety function shall be of cyclic running with determined cycle interval irrespective of the events.

c) In the processing of the measured, reported data the operational system or the programme module of the running environment shall not be involved. The data coming from the supervised process shall have no effect on the behavior of the operational system or the running environment.

d) The change of the incoming data values shall not be managed by programme interruptions.

e) The change of the incoming data values shall not affect the operation instruction of the tasks of the user, operational system or the running environment.

f) The connection with the outside world of the processor of the one-processor system or, in the case of several processors, the workload of the data channel between the processors shall be permanent and it shall not be dependent on the values of the processed data or the failure status of other parts of the system.

g) The distribution of the system's resources shall be determined at the design stage and it shall not change dynamically.

h) The hardware and software modules and their connecting overlays shall be strictly determined.

i) The software and hardware modules shall be classified and tested irrespective of their application and before the application as well.

j) In order to avoid the accumulation of effects induced by hidden failures and their appearance as a common cause failure the subsystems of the system carrying the redundancy or diversity shall be of asynchronous operation to each other, their synchronizing mechanisms shall be avoided at the design and the operational phases.

k) The deterministic operation of the system shall be demonstrated by theoretical considerations and testing during the lifecycle and the introduction of possible modifications.

l) The effects of occurring failures induced despite the compliance with correct design principles, shall be minimized by the application of failure-proof hardware and software solutions, and of the principle of operating safely. During the minimization the consequence of the missed operation of safety functions shall be compared with the

consequence of inadvertent operation due to the operating safely, and the decision shall be made for the lower risk.

m) The possibilities of failures expected in the hardware and software functions theory and/or those which may occur with higher probability than 10^{-2}/year based on the existing failure statistics, shall be detected by automatic or operator initiated testing, of period intervals adjusted to and aligned with the required induced reliability of the system. This requirement shall be met even if the possibilities of failures are covered by operating safely, since the inadvertent operation of safety function shall be avoided as well.

n) The internal common mode failure possibilities shall be minimized by diverse solutions of the hardware and software architecture in line with the ALARP principle to the extent which is still in agreement with the principle of simplicity and the transparency of the internal functions of the system performing safety function. (NSC Volume 3, Section 5.100.)"

The design of programmable systems and equipment classified into ABOS 2 safety class should be performed by considering the legal requirements of paragraphs a-n), based on the specification related to the hardware and software systems. The applied design considerations and technical solutions should be justified by safety analysis, the requirements for the system and equipment should be included in the design specification.

Relevance of considering the design requirements should be examined also for ABOS 3 safety class systems and equipment.

„If a component selected for a certain function is programmed in itself, but the programme burnt-in during production only exists together with the carrier hardware (firmware) and is readily available, and in the given task can be applied in line with the unchanged characteristics based on the design specifications, without modifications, then this system component shall be managed as a traditional control engineering element. Only such in-production burnt-in software can be used which are produced in large series under controlled circumstances and as an asset is provided with appropriate reference." (NSC Volume 3, Section 5.101.)

Handling of the programmable tools as traditional instrumentation and control element should be justified by the compliance with the criteria specified in the requirement. In the design task only such tools should be applied, for which it can be justified that compliance with the requirement

for production and the acceptability can be justified by assessable reference data.

„The four components of the computer based system shall be designed separately, taking into account the specifications valid for the boundary interfaces and the characteristics of the component lifecycle. These four components are the following:

a) The software realizing the planned functionality (including the technological and communication functions), hereinafter referred to as software.

b) The operating system responsible for the co-operation of the software and hardware.

c) The hardware providing resource for the software and the operating system.

d) The interface tools between the technology and user, resulting system component as the embodiment of the previous three points, like the measurement chains, manual control assets, traditional displays and auxiliary instruments, hereinafter referred to as the traditional control engineering elements." (NSC Volume 3, Section 5.102.)

The design of the main separation components of programmable systems or equipment should be performed based on the unified system specification covering the whole system, but following the design specification of the given component. Compliance with the specification should be justified.

„In the systems, system components classified into the ABOS 2 safety class only tested, unique or type-qualified hardware elements can be used." (NSC Volume 3, Section 5.104.)

In the ABOS 2 safety class, during the design task only hardware elements qualified and certified by independent qualification institute should be applied, which requirements should be included in the design specification. In the selection the compliance with the criteria should be examined and justified. In the case of application of individually developed hardware elements (current circuit) the adequacy of the circuit should be justified by inspection documentation issued by independent qualification institute. The qualification documents should be attached to the design documentation of the system.

"In the systems, system components classified into the ABOS 3 safety class it is recommended to use elements validated in the testing environment specified for the given task, but the following shall be taken into account:

a) *Use of the shelf modules with appropriate reference, coming straight from the manufacturer.*

b) *If a module, performing unique function is required only modules with appropriate reference, manufactured by the producer can be used.* (NSC Volume 3, Section 5.105.)

In the design of systems and equipment classified into safety class the licensee should apply only such hardware and software (operating system and user software) elements, the adequacy of which have been justified in appropriate testing environment. In the ABOS 3 safety class deviation is possible from the design requirements in that sense the qualification is acceptable by the description of the reference data (manufacturer and product). In the selection of the hardware and software elements the compliance with the requirement should be examined and justified. The qualification documents should be attached to the design documentation of the system.

"In the system components, classified into the ABOS 2 safety class only such operational systems can be used which have been validated in the testing environment specified for the given task." (NSC Volume 3, Section 5.106.)

In the design of the system components and equipment classified into ABOS 2 safety class such hardware and software elements should be used, the adequacy of which have been justified in a testing environment commensurate with the application. The prescription highlights the importance of the requirement for operating systems. Compliance with the criteria should be justified during the design; its documents should be attached to the design documentation. The requirements should be included in the design specification of the system.

"In the systems, system components, classified into the ABOS 3 safety class it is recommended to use operating systems which have been validated in the testing environment specified for the given task, but at least it is necessary that it shall be a robust operating system originating from a manufacturer having appropriate reference and significant operational experience and if it is complex then it shall be capable of creating configurations for the given application (which means comprising important and actually used components from the application point of view)." (NSC Volume 3, Section 5.107.)

In the design of the operating system of systems and equipment classified into ABOS 3 safety class only such software should be applied, the

compliance of which have been justified in a testing environment commensurate with the application. The prescription highlights the importance of the requirement for operating systems. Compliance with the criteria should be justified during the design; its documents should be attached to the design documentation. The requirements should be included in the design specification of the system. Deviation is possible from the design requirements if the compliance is acceptable by the description of the reference data (manufacturer and product).

Based on the legal requirement robust operating systems should be applied in the ABOS 3 safety class. Also robust operating systems should be applied in the ABOS 2 safety class, as appropriate.

Compliance with the requirements should be justified during the design task; its documents should be attached to the design documentation. The requirements should be included in the design specification.

„In the system components classified into the ABOS 2 safety class only such software can be used which is a validated software for the testing environment designed, verified and specified for the given task or such software can be used, which consist of modules justified in the same manner. The method and procedure relevant to the justification of the identification of application and functionality requirements shall be designed." (NSC Volume 3, Section 5.108.)

During the design of ABOS 2 safety class systems and equipment only such hardware and software elements should be applied, the compliance of which have been justified in a testing environment commensurate with their application. The prescription related to the user software should highlight the importance of the requirement.

By the consideration of the characteristics of the application the compliance with the requirements should be justified.

The compliance with the requirements should be justified during the design task. Its documents should be attached to the design documentation. The requirements should be included in the design specification of the system.

In the systems, system components, classified into the ABOS 3 safety class it is recommended to use operating systems which have been validated in the testing environment specified for the given task, but it is possible to use applications made by systems having appropriate reference, if the experience statistics, reference data are available related to the developing system. It is possible to use uniquely developed software made with the help

of the application of the programme language and its interpreter having the appropriate reference. It is a design requirement in every case to develop the method and procedure relevant to the verification of the identification of application and the planned functionality requirements." (NSC Volume 3, Section 5.109.)

The design or selection of user software of systems and equipment classified into ABOS 3 safety class only such software elements should be used, the compliance of which have been justified in a testing environment commensurate with their application. The prescription related to the user software should highlight the importance of the requirement. Deviation is possible from the requirements if the compliance is unambiguously acceptable by the description of the reference data, manufacturer, product, development environment.

By the consideration of the characteristics of the application the compliance with the requirements should be justified.

The compliance with the requirements should be justified during the design task. Its documents should be attached to the design documentation. The requirements should be included in the design specification of the system.

"In the systems, system components, classified into safety classes only such software can be used which have been verified and validated in the testing environment specified for the given task." (NSC Volume 3, Section 5.110.)

The prescription reinforces the above discussed legal requirements. In programmable systems and equipment fulfilling safety function such software should be applied, the compliance of which is unambiguously justified by the application of verification and validation procedures. The compliance with the requirements should be justified. Its documents should be attached to the design documentation. The requirement, together with the requirements related to verification and validation, should be included in the design specification of the system.

The components of systems, system components classified into safety classes (hardware, software, operating system, traditional instrumentation and control engineering elements) shall be tested separately and together comprehensively in the given environment. It is obligatory to design the testing and the acceptance criteria. (NSC Volume 3, Section 5.111.)

The prescription may be interpreted by the extension of the requirement 5.110. In programmable systems and equipment fulfilling safety function such software should be applied, the compliance of which is unambiguously

justified by the application of verification and validation procedures. The verification and validation procedures are preliminary designed.

The requirements for the implementation of verification and validation procedures and for the elaboration of inspection programs should be included in the design specification of the system. The inspection programs should be justified by safety analysis.

"The achievement of the characteristics required above for components classified into ABOS 2 safety class should be justified by an independent expert, yet in the design stages." (NSC Volume 3, Section 5.112.)

In the ABOS 2 safety class the compliance with and adequacy of the design requirements related to the programmable systems and equipment fulfilling safety function should be justified by independent expertise. The opinion of the independent expert should be attached to the design documentation of the system. The independent expertise can be acceptable if the requirement for the independence is met, and the opinion is based on the actual and real design documentation of the system and equipment.

According to the general requirements the design process should be defined by considering the licensing obligations. The activities should be scheduled such a way that for the time of licensing procedures the plans and justifications supporting the application are available (NSC Volume 3, Section 3.001.). The requirements for the licensing process are included in Chapter 6 of Volume 1 of the Nuclear Safety Code, and within that the details corresponding to the design phase are prescribed in the Chapters 6.2, 6.3 and 6.4. (modification license in principal, manufacturing license, acquisition license). In order to meet the related prescriptions the licensee should describe the following in the design documentation as minimum:

1. reason, justification for modification,
2. list and classification of components,
3. applied standards and recommendations,
4. design specifications and the related designer considerations,
5. examination of compliance with design requirements specified in the laws, safety justification (safety plan) of design specification (requirements),
6. deviations from modification license in principal, and their justification,

7. list of regulatory licenses and prescriptions corresponding to the design task, justification of meeting the regulatory requirements,
8. technical description,
9. functionality of the system, equipment and their components,
10. dimensioning information of hardware elements,
11. construction designs corresponding to manufacturing, establishment or modification,
12. documentation, qualification documents of hardware and software components of safety programmable systems,
13. methods and tools of code generation, operating parameter and process code modification, technical and administrative rules for their implementation, safety justification of acceptability of the methods,
14. justification of acceptability of the applied technical solutions,
15. scope of operative modifications (e.g. operational parameter modification), and safety justification of implementation possibility of these activities,
16. validation and verification (V&V) plan related to the software development process,
17. documentation and qualification documents of the software development environment,
18. design and implementation process, scope of inspections planned for the demonstration of meeting the requirements, features and acceptability of inspections,
19. factory acceptance test corresponding to the compliance with the requirements,
20. rules of implementation becoming necessary during the manufacturer inspections, basic principles of determination of the inspection activities corresponding to the modification,
21. documentation of factory acceptance test equipment, justification of acceptability of equipment,
22. demonstration of compliance with those design requirements, for which the demonstration can be implemented already in the design phase,

23. operating state of the unit, systems and equipment concerned in the modification during the implementation, justification of acceptability of the design operating states,
24. declarations justifying the consideration of prescriptions and requirements,
25. independent expert declaration,
26. designer recommendations related to operation and maintenance,
27. requirements and justification for the designer, manufacturer and implementor,
28. documents justifying the designer and manufacturer qualification,
29. schedule of implementation,
30. examination of modification of the Final Safety Analysis Report,
31. examination of modification of the Technical Specifications,
32. scope of documents necessary to be modified,
33. training needs.

Identity of design and licensing documents should be ensured.

4.3.2. Application of standards

The most important specific standards related to the design of programmable systems and equipment fulfilling safety function are as follows:

1. IEC 60880: Software for Computers in the Safety Systems of Nuclear Power Stations
2. IEC 60987: Programmed digital computers important for safety for nuclear power stations
3. IEC 61226: Nuclear power plants - Instrumentation and control systems important for safety - Classification
4. IEC 45A/359/NP.1999. Nuclear power plants – Instrumentation & Control – Computer based systems – Software aspects of I&C systems important to safety of class 2 and 3
5. IEC 60122: Software for Computers in the Application of Safety-Related System

6. IEEE 730: Software Quality Assurance Plans
7. IEEE 829: IEEE Standard for Software Test Documentation
8. IEEE 830: IEEE Guide to Software Requirements Specifications
9. IEEE 1008: IEEE Standard for Software Unit Testing
10. IEEE 1012: IEEE Standard for Software Verification and Validation Plans
11. IEEE 1016: IEEE Recommended Practice for Software Design Description
12. IEEE 1028: Software Reviews and Audits