

AN INTEGRATED RISK INFORMED DECISION MAKING IN THE NUCLEAR INDUSTRY

Mieczysław Borysiewicz¹, Karol Kowal¹, Piotr A. Prusiński¹, Marcin Dąbrowski²

¹National Centre for Nuclear Research (NCBJ), Nuclear Energy Department, Nuclear Energy Division, Poland

²National Atomic Energy Agency (NAEA), Department of Nuclear Safety, Division of Inspection of Nuclear Installations, Poland

Abstract. *The regulatory body, established to ensure safety of nuclear facilities, is expected to make right decisions and provide appropriate regulations for the nuclear industry. The traditional manner of its activity has been based on a deterministic approach to safety analyses. However, increased maturity of Probabilistic Safety Assessment (PSA) makes it complementary to deterministic studies. The new IAEA concept, described in this article, is to apply an integrated approach by combining both deterministic and probabilistic insights with other requirements affecting the decision making process.*

Keywords: Nuclear Safety, Integrated Risk Informed Decision Making (IRIDM), Probabilistic Safety Assessment (PSA), Deterministic Safety Assessment (DSA)

ZINTEGROWANY PROCES DECYZYJNY UWZGLĘDNIAJĄCY RYZYKO W PRZEMYSŁE JĄDROWYM

Streszczenie. *Organ regulacyjny, powołany w celu zapewnienia bezpieczeństwa jądrowego, jest odpowiedzialny za podejmowanie decyzji i wprowadzanie rozporządzeń dla przemysłu jądrowego. Tradycyjny sposób jego funkcjonowania opiera się na deterministycznym podejściu do analiz bezpieczeństwa. Rozwój analiz probabilistycznych (PSA) sprawia jednak, iż są one traktowane jako podejście komplementarne. Nowa koncepcja IAEA, opisana w tym artykule, polega na zintegrowanym podejściu, uwzględniającym analizy deterministyczne, probabilistyczne i inne aspekty procesu decyzyjnego.*

Słowa kluczowe: bezpieczeństwo jądrowe, proces decyzyjny, ryzyko, probabilistyczne analizy bezpieczeństwa (PSA), deterministyczne analizy bezpieczeństwa (DSA)

Introduction

All over the world a nuclear industry structure is organized in a similar manner, meaning its stakeholders are usually: regulatory body, utility (investor) and technology vendor. The utility, owning or operating a nuclear power plant (NPP), is responsible for its safety throughout its lifetime, which means effective control of nuclear radiation, radioactive waste and its transport within the country. For this purpose a nuclear law has to be enacted first and a regulatory body has to be established to enforce the law and to control if the law is obeyed by nuclear facility operators [12].

The major regulatory body responsibilities and functions can be briefly described as authorization, review and assessment, inspection and enforcement, and development of regulations and guides [24]. Authorisation means granting a written permission by the regulator for an operator to perform specific nuclear activities, based on the national legislation, which includes, for example, necessary licensing, certification and registration. After the authorisation process, the operator of the nuclear facility is continuously supervised by the regulatory body, which determines whether the operator's activity ensures that the facility complies, throughout its life cycle, with the safety objectives, safety principles, and safety criteria approved by the national regulations. The regulatory body conducts inspections to check independently and satisfy itself that the operator is in compliance with the requirements set out in the authorization and regulations. If non-compliance with conditions of the authorization is demonstrated the regulatory body applies appropriate sanctions against the operator, including cancelation of the licence for nuclear activity. Consequently, development of appropriate regulations and guides plays a crucial role in the context of the relationship between nuclear facility operator and regulatory body. These documents are created by the national regulatory authority regarding the indications and standards provided by the International Atomic Energy Agency (IAEA) headquartered in Vienna, Austria.

However, the role of the IAEA is limited to support, not to supervise, the regulation development process in the Member States. Thus the regulatory body is responsible for the nuclear law within the country, while the IAEA provides only the general safety standards and indications that can be adopted by the national authority. These standards are issued as the Safety Standards Series and categorised into Safety Fundamentals, Safety Requirements and Safety Guides. Moreover, the reports on safety in nuclear facilities and activities are issued in other publication series, in particular the Safety Reports Series, the Technical Reports Series, the Training Course Series etc. While sets

of the IAEA reports aim to prevent accidents, there are also publications on security issues developed as the Nuclear Security Series, which goal is to reduce the threat of terrorist acts causing intentional damage to the nuclear facility. Since interfaces between safety and security issues exist, appropriate measures have to be taken to achieve both objectives in an optimal manner [35].

Besides of a good legislation, the regulatory body is expected to consider results of specialised safety analyses, performed in order to support decision making process on both new reactor licencing and nuclear safety of existing facilities. Making right decisions in this field is in fact the mission of the regulatory body, which is established to ensure that the safety of the public and of the operating staff of nuclear facilities is protected [22]. Although, the regulatory body usually has an internal group qualified to prepare some of required safety studies, it is a common practice to delegate the whole safety evaluation to the independent organization which, from now on, gains status of the Technical Support Organization (TSO). However, in any case when the TSO performs safety analysis on the request of the regulator, the final decision and ultimate responsibility always lies in the competences of the President of the regulatory organization. Thus the regulatory body never delegates its competences in the decision making on nuclear safety to any external organization including TSO. The role of TSO can be played either by one or several institutions i.e. university laboratories, nuclear research centres and all other units qualified to perform regularly the comprehensive assessments of nuclear safety or even independent specialists in the relevant fields if necessary. Thus the TSO model can be slightly different, depending on the country, while its main tasks in supporting the regulatory body usually stay the same all over the world. Besides of safety assessment, TSO can also assist in developing nuclear regulations, conducting technical inspections and, in case of an accident, it is expected to advise on the possible countermeasures [5, 6, 9].

Although, in some countries it is allowed to provide technical support for both the regulatory body and the utility at the same time and by the same organization, in general it is not recommended due to additional requirements that have to be fulfilled, i.e. political and economic independence of TSO has to be ensured. Therefore TSO should be required to demonstrate that there are no conflicts of interest in its activity. Moreover, it usually means that no one of TSO staff should work for both parties in the same subject area so as to avoid reviewing one's own results and guarantee independence of the analysis. Therefore, it is a good practice to delegate different persons and choose the alternative methods to be used for the two sides [15].

However, it is the most transparent way to establish two separate TSO structures, one for the regulator and another one for the utility.

Another issue is the role of TSO in public information and social debate transparency, especially during licensing of new reactors and nuclear power plant construction. These activities have always been of special interest to the media and the public opinion because of risks associated with their implementation. Public debate is recognized as an important, thus the TSO could participate in an open discussion next to the Government, local decision making bodies and other groups of interest. Nevertheless, it is crucial for TSO to maintain its neutrality and independence. Therefore, its role in the public debate is somewhat limited e.g. it cannot argue in favour of or against any specific solution or concept [15]. On the other hand, the TSO is able to supply the background information for both the decision makers and the public. In particular, the decision makers should be well informed about risks associated with various options to choose from, when it comes to the nuclear safety assurance.

1. Perception and evaluation of the nuclear risks

How people view risks and apply value judgments seems to be the most challenging factor of the decision making based on risk. The way we all treat risks depends on our perception of how they relate to us and the things we value. It has been found that there is a wide range of factors influencing this perception. Particularly important for man-made hazards are: how well the process (giving rise to the hazard) is understood, how equitably the danger is distributed and how well individuals can control their exposure and whether risk is assumed voluntarily [19].

Many researchers argue that the concept of risk is strongly shaped by human minds and culture. It may include the prospect of physical harm and other factors, such as ethical and social considerations, and even the degree of trust in the ability of those creating the risk (or in the regulator) in ensuring that adequate preventive and protective measures are in place for controlling the risks. For many new hazards, high quality risk assessments by leaders in the field often fail to reassure people even using all available data and best science and technology. The other thing is that many of risk assessments cannot be undertaken without making a number of assumptions such as the relative values of risks and benefits or even the scope of the study.

The studies have established that hazards give rise to concerns which can be put into two broad categories: the individual and societal. The individual concerns relate to how individuals see the risk from a particular hazard affecting them and things they value personally. Individuals may be willing to live with a risk that they do not regard as negligible, if it secures them or society certain benefits, they would want such risks to be kept low and clearly controlled. Societal concerns cover the risks from hazards which impact on society and which, if realized, could have adverse repercussions for the institutions responsible for putting in place the provisions and arrangements for protecting people, e.g. Parliament or the Government. This type of concern is often associated with hazards that give rise to risks which, were they to materialize, could provoke a socio-political response, e.g. risk of events causing widespread or large scale detriment or the occurrence of multiple fatalities in a single event. Typical examples relate to nuclear power generation, railway travel, or the genetic modification of organism.

In order to specify the safety goals in a quantitative manner, concrete numerical values describing the level of different risk indicators have to be evaluated first. For that purpose the common concept of risk must be expressed in more mathematical terms. Thus the generally accepted definition of risk is described by the equation below:

$$R_i = P_i \cdot C_i, \quad (1)$$

where R_i is the risk associated with an accident sequence i , while P_i describes the probability of the sequence i and C_i specifies

the magnitude of the consequences corresponding to its occurrence.

When the consequences from an accident sequence i can be specified by a continuum of outcomes between x and $x + \Delta x$, the risk density $R_i(x)$ of magnitude $C_i(x)$ can be defined [10].

In such a case usually more important becomes the risk of damages exceeding the acceptable magnitude $C_i(X)$. This risk is the complementary cumulative distribution function for accident sequence i , described by the equation below:

$$R_i(\geq X) = P_i \sum_j \int_x^{\infty} C_{ij}(x) dx, \quad (2)$$

where $C_{ij}(x)$ includes a variety of predicted consequences of type j caused by the event sequence i . This factor is especially important in the case of severe release of radioactivity, when more than one type of potential damage could occur and they all have to be taken into account during the nuclear risks management [10].

Risks, generated by nuclear facilities, can be analyzed in details by making use of PSA (Probabilistic Safety Assessment) methodology. It includes identification of possible initiating events leading to the potential accident, specification of expected accident scenarios as well as an estimation of their probability and consequences. The PSA methodology has been elaborated in the 70's and it is being used and developed until now [38]. By using these methods the individual and societal risk profile of installation can be obtained and compared with current standards and required criteria [2, 21, 39].

It should be emphasised that the individual risk estimation is to calculate the risk to any individual who lives within a particular distance from a plant; or who follows a particular pattern of life that might subject him or her to the consequences of an accident. In making such an estimate the first question concerns how likely is an accident in the first place, and for this it is necessary to consider the likelihood of each important kind of plant failure. Data on the reliability (i.e. failure rates) of plant and particular components are collected and computerized to assist in such studies. Account has to be taken for the reliability of human beings in the design, construction, testing, operation, maintenance, and modification of such plant and components. Then the results of particular failures, e.g. how much toxic gas, or flammable substance, or radioactivity would be released, have to be considered. It is then necessary to calculate how such releases would be likely to affect a hypothetical person who was at some particular spot, taking account of the possibility that he or she might be in or out of doors; what dose would be received, and what harm would this do. Such calculations have also to take account of the behaviour of substances under different weather conditions. Population and sometimes transport patterns have to be considered. Finally, the chances of harm from all significant failure causes have to be summed up to give the overall level of risk from the installation. Only when such complex studies and calculations have been made it is possible to predict the chance that any individual living within a particular radius, or behaving in a certain way, will be injured by an accident. Such calculations are referred to as individual risk calculations, and enable us to say things like a person who lives within half a mile radius of such and such a plant has a chance of x per annum of being injured from an accident at the plant.

According to the different forms of hazard for which calculations are made, there are various possible ways in which people might be injured. They might die more or less instantaneously from the effects of explosions, fire or toxic gas release. Radiation is a different case, since unless the dose is extremely large death within a few weeks or even years would be extremely unlikely. What could happen is that, depending on size of the doses, a proportion of the people receiving them would develop a cancer some years after the exposure took place or possibly pass on a genetic abnormality to some of their descendants (a number of non-radioactive chemicals can cause the same sort of effects). So, by and large, the risk that an individual experiences from radiation exposure is to increase somewhat that person's chance later in life of developing a cancer,

which might or might not be treatable. This needs to be borne in mind when comparing the effects of exposure to ionising radiation with the effects of conventional accidents, which are immediate.

To estimate large events, we use the term societal risk, and in doing so, we have to consider not only the many different forms an accident could take, but the multiple consequences involved and their cost or severity. In principle at least, the different forms of harm that could follow from a very large accident could be added up and given a money value, provided of course that one is prepared to attach a value to the loss of human life [18].

Then effectiveness of engineered safety systems, their reliability as well as adequacy of safety procedures and countermeasures availability can be assessed. Moreover, the main weaknesses of nuclear systems and the most probable sequences of undesired events can be also identified early at design and pre-commissioning stage, which gives a chance to successfully preventing their occurrence during plant operation. It should be noted that some engineering aspects important to safety may not be explicitly addressed in the safety analysis. For some of these aspects, no well-defined acceptance criteria are available and therefore the assessment of the compliance with the safety requirements is based on a good engineering judgement.

2. Safety assessment for facilities and activities

In general ensuring safety of nuclear installations and activities is reducing to acceptable level the radiation risk for people and environment, they generate during their whole life cycle. Comprehensive safety assessment is an indispensable mean facilitating to achieve this goal. IAEA set up 24 principles for recommended safety assessment including its goal, scope, procedures and uses [32]. In particular the principles state the following:

- The responsibility for carrying out the safety assessment shall rest with the responsible legal person, i.e. the person or the organization responsible for the facility or activity.
- The primary purposes of the safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, in compliance with the requirements for radiation protection and safety as established in the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, have been fulfilled.
- The results of the safety assessment shall be used to specify the programme for maintenance, surveillance and inspection; to specify the procedures to be put in place for all operational activities significant to safety and for responding to anticipated operational occurrences and accidents; to specify the necessary competences for the staff involved in the facility or activity and to make decisions in an integrated, risk informed approach.

Figure 1 shows the main elements of the safety assessment process. Before proceeding safety assessment, proper setup has to be prepared, which includes ensuring the necessary resources (e.g. sufficient number of specialists and adequate funding), information (e.g. details of design and construction of the facility) and analytical tools (e.g. computer codes for carrying out the safety analysis). Moreover the safety limits must be defined in the national regulations in order to assess if the safety of the facility or activity is adequate or not.

After the preparation process there are several features to be assessed including the possible radiation risks associated with the facility or activity, all relevant safety functions performed to prevent or mitigate the consequences of undesired events, site characteristics relating to the safety, available measures in place to protect people and the environment from harmful effects

of the ionizing radiation as well as some engineering aspects (e.g. quality of safety related equipment) and possible human errors.

The safety assessment covers also checking whether the basic safety principles, like defence in depth (DID) philosophy, safety margins and multiple barriers rule, are efficiently implemented. All these aspects will be described in details and discussed in this article in the context of the decision making process.

Another part of the safety assessment are the safety analyses. The full range of undesired initiating events, that could occur over a broad range of operational states (including different levels of availability of the safety systems), is addressed in such studies (Tab. 1). In general there are two complementary methods to perform them: the deterministic (DSA – Deterministic Safety Assessment) and probabilistic one (PSA). The major objectives and methodology as well as differences and limitations of this two approaches will be analyzed in this paper. However, regardless of approach these analyses aim to verify whether facility or activity is in compliance with safety criteria, defined by the national regulations and the regulatory body requirements.

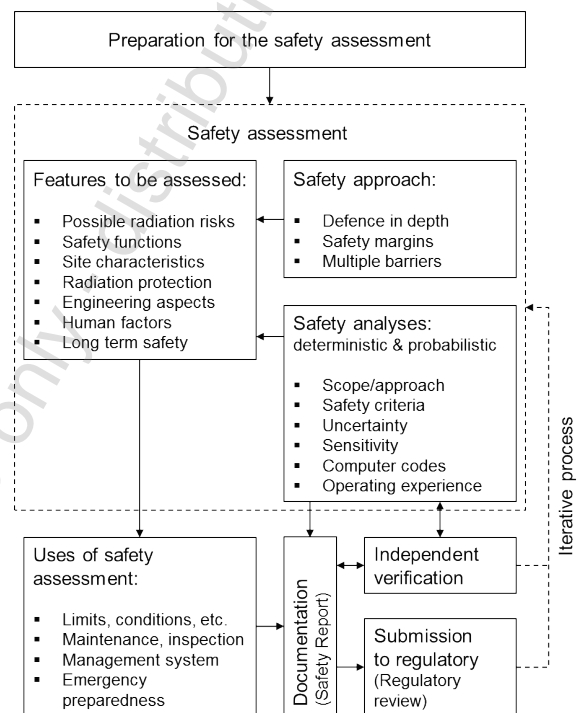


Fig. 1. Overview of the safety assessment process [cf. 32]

Table 1. Possible subdivision of postulated initiating events [31]

Occurrence (1/reactor year)	Characteristics	Plant state	Terminology
10 ⁻² – 1 Expected over the lifetime of the plant	Expected	Anticipated operational occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions
10 ⁻⁴ – 10 ⁻² Chance greater than 1% over the lifetime of the plant	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions
10 ⁻⁶ – 10 ⁻⁴ Chance less than 1% over the lifetime of the plant	Unlikely	Beyond design basis accidents	Faulted conditions
< 10 ⁻⁶ Very unlikely to occur	Remote	Severe accidents	Faulted conditions

The deterministic analyses (DSA) require determination of the minimum margins to the acceptance criteria for each group of postulated initiating events and sequences. Then an adequate set of conservative or best estimate assumptions for the initial and boundary conditions should be used.

This type of safety analysis covers only those combinations of transients whose frequency remains the design basis accidents. Thus the time span of any considered scenario should extend up to the moment when the plant reaches a safe and stable end state.

The PSA studies provide estimations of both probability and consequences of an accident scenarios possibly leading to the core melt and radiological releases to the environment i.e. for beyond design basis accidents and severe accidents.

Results of these studies should be additionally verified by the independent organization in order to ensure that there are neither oversights nor mistakes. In general, after verification process the results of deterministic studies complemented by some PSA results on beyond design basis accidents and severe accidents are included into the overall Safety Assessment Report (SAR). This report contains also another important conclusions from the safety assessment on limits and conditions of the facility operating or the carried out activity, maintenance schedule, management and emergency preparedness.

The SAR, when completed, is then submitted to the regulatory body, authorized to its acceptance, rejection or to request additional revisions. Without acceptance of the SAR any nuclear facility cannot operate and nuclear activity can no longer be carried out. This is also a condition for successful completion of the licensing process of new installations and activities to be launched in the future.

3. An integrated risk informed decision making

The fundamental objective of nuclear safety assessment is to protect people and the environment from the ionizing radiation. For that purpose the risks associated with nuclear power plants, throughout their life cycle, must be maintained as low as reasonably practicable. It means minimizing the radiological exposures from normal NPP operation, preventing potential nuclear accidents and mitigating the consequences when they occur. Moreover, the design weaknesses, can be identified before the nuclear power plant construction. It gives a chance to abandon technology, which does not meet the specified requirements and thereby does not provide appropriate safety level.

Since there are various factors affecting the safety of nuclear power plants, different techniques are used to assess the risks associated with them. The traditional approach to safety analysis is based on the deterministic principles, that underlies the design and operation of the nuclear power plants. Its philosophy is to ensure that the design is fault tolerant, to adequately meet a defence in depth rules, to emphasize safety acceptance criteria and to maintain adequate safety margins even during a postulated system failures. Finally, the objective of deterministic safety studies is to demonstrate that the designed barriers will prevent an uncontrolled release of radioactive materials to the environment for all plant states assuming the conservative approach [31].

Nevertheless, there are also safety issues requiring both the deterministic and probabilistic assessment. As an example, equipment qualification of nuclear power plant components can be discussed. It must be demonstrated, basing on deterministic approach, that the performance of equipment required to survive design basis accidents, is adequate [31]. In order to be sure that the systems and components crucial for nuclear safety will perform their function properly, according to the design both under normal operational conditions as well as during an accident, it is necessary to check their resistance to the accident conditions [14]. This activity is one of the defence in depth methods for protection against the release of radioactive materials and preventing failures of equipment due to hazardous service conditions, e.g. high temperature, humidity and radiation fields or high vibration due to earthquake. Moreover, the time

of exposure and the ageing process of equipment should be also taken into account in that kind of analysis [20].

However, while the deterministic analysis answers question if the safety margins are retained during a postulated accident, the probabilistic approach is able to predict the occurrence frequency of such an accident. Therefore, the probabilistic assessment of equipment failure frequency has been recognised as an important factor of the qualification process next to the deterministic study. Furthermore, the priorities for equipment qualification may be dictated by the predicted consequences of specific component failures and their impact on overall nuclear safety. These factors could be assessed by probabilistic methods to identify the increase of public risk as a result of the postulated failures [20].

Nowadays, there is a general consensus that the Probabilistic Safety Assessment has reached the status of methodology mature enough to strongly influence the design and operation of nuclear power plants. It is being used to complement the deterministic approach and to provide additional insights that would not otherwise be available. Therefore, it is believed that its usage by regulatory bodies in the risk informed regulation concept can result in reduced threat for the public health [29]. Thus the international standards indicate that the results of the safety assessment have to be used in order to make decisions in an integrated, risk informed approach, by means of which the results from the deterministic studies, probabilistic insights and any other requirements are combined in making decisions on safety matters in relation to the nuclear facility or activity [32]. An integrated risk informed decision making process (IRIDM), if performed in balanced and comprehensive manner, should bring transparency and auditability to complex decisions. However, its applicability depends strongly on appropriate integration of a number of differently weighted elements [36].

The IRIDM process has been originally defined as a modern, systematic approach to identification and balanced integration of the major contributors influencing nuclear power plant safety [36]. However, the universality of its methodology makes it applicable to all types of nuclear facilities and activities that give rise to radiation risks, including research reactors, nuclear installations as well as the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste. Additionally, the IRIDM process has been recognised as a flexible tool, which after appropriate adjustments, can be successfully applied to the non-nuclear technological installations [3].

The main concept of the IRIDM process has been developed in order to support utilities and regulatory bodies in both making right decisions on safety issues for nuclear facilities as well as prioritising their own tasks, according to the significance of risk associated with different fields of their activity.

In case of plant operators there is an additional reason of their interest to the IRIDM methodology implementation in the management process, economical optimisation of their activity. However, the transparency of this approach to decision making and the explicit consideration of risk, makes the IRIDM process useful for the international nuclear community as a whole, including designers, suppliers, licensees, operators and technical support organizations.

Usually, when an unique, non-routine decision on safety matters in relation to the nuclear facility or activity has to be made, qualitatively different insights must be taken into account together, including deterministic and probabilistic outcomes, regulatory requirements, economic, social and other safety important factors. Additionally, application of these approach to physical security is now being considered by the international community.

Finally, one can define the IRIDM process as a comprehensive way of making decisions about modifications of the design or procedures, which are related to safety of nuclear facilities and activities, as well as changes in the security systems in order to reduce the impact of a terrorist threat. Safety and security issues, when considered together in an integrated manner, should

lead to coherent solutions, which means that enhancements made in these areas cannot adversely affect, but assist each other.

Moreover, the integrated approach to the decision making process seems to be especially useful in such cases, when there is a number of different options leading to acceptable results. Then the risk informed analysis of multi attribute safety, security and regulatory issues is powerful enough to identify the expected optimum solution.

4. Basic framework and key elements of IRIDM

Since the general idea as well as the main objectives of the risk informed approach to decision making seem to be clear and reasonable, the formal framework of this process is needed to identify and describe in details the interrelations between its key elements. The implementation of a commonly known scheme of the decision making allows to review the fact-based grounds of once made decision and, if required, its reconsideration.

4.1. Characterization of the issue

According to the basic framework, describing the IRIDM process (Fig. 2), the clear and unambiguous definition of issue to be resolved is crucial to identify which elements or information are relevant to making a decision. The issue characterization should provide additionally its necessity evidence as well as an impact on the facility operation and safety, which covers required design changes, security arrangements, organizational model, internal procedures, man-machine interactions and other factors, that potentially might be dependent on the decision related to the considered matter.

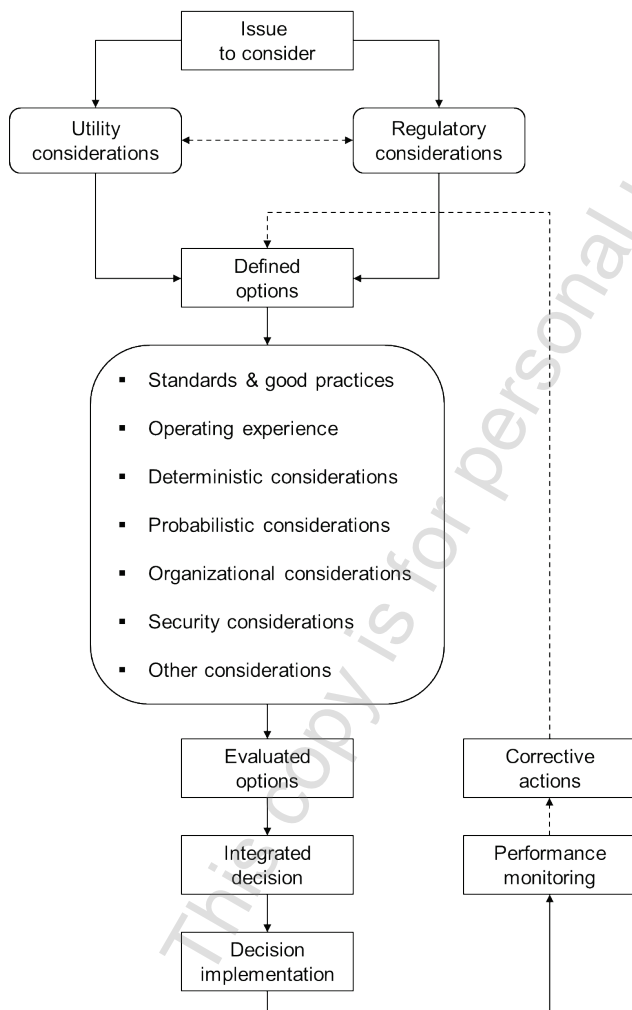


Fig. 2. Organizational framework and key elements of the IRIDM process [cf. 36]

4.2. List of options to choose from

After defining the problem, consideration must be given to the requirements of both regulatory body and licensee in order to draft a preliminary set of options, that potentially could solve the issue. However, to make the final decision and choose one from the preliminary set of options, specified inputs must be established, namely the standards and good practices, operating experience, deterministic and probabilistic considerations, organizational and security systems and other factors such as research or economic insights. Relative importance of each element depends upon the decision to be made and should be weighted either qualitatively or quantitatively. This process leads to evaluation and to reduction of the preliminary set of options. Finally one of them should be chosen, implemented and monitored. If the performance of just implemented decision is not satisfactory corrective actions should be undertaken and the list of options needs to be redefined.

4.3. Standards and good practices

The basic principle of decision making is the compliance with legal requirements in any case under consideration. Thus the national legislation, including the regulatory requirements, must be strictly respected. Besides of mandatory regulations there are also generally accepted international standards and procedures, developed by professional bodies like government agencies or engineering organizations. These standards are usually based on the long operating experience and practical implementations of IRIDM. In such a way best practices are described and published in the form of official guidance and their considerations has been recognized as a major factor in many IRIDM activities.

4.4. Operating experience

The operating experience is also important in the context of the consequences prediction. Lessons learned from the undesired events that have occurred at the nuclear power plant itself or at the similar facilities provide the information what can happen and how to prevent it. This knowledge is applicable in all other IRIDM inputs assessment, including both deterministic and probabilistic insights as well as the organizational, security, research and economic considerations [23, 26].

4.5. Deterministic considerations

The deterministic principles, that underlie the safety design and operation of nuclear facilities, require firstly the definition of safety criteria to be meet, secondly the appropriate level of defence in depth to be guaranteed and finally large safety margins to be ensured. The safety criteria mean a set of values, describing crucial parameters and performance of the nuclear installations, in compliance with which its safety is justified e.g. maximum acceptable peak cladding temperature of the fuel rods. These requirements cover also the limits of the radiological doses for the operating staff and for the public as a whole, which cannot be exceeded. In order to determine whether the predefined IRIDM options meet all deterministic acceptance criteria, established by the regulatory documentation, the design basis accident (DBA) analysis must be performed [21, 36, 37].

The DBA analysis starts from postulating a set of initiating events, which – if occur – could potentially lead to a nuclear accident. Then the different accident scenarios are verified in the context of the design capability for protecting against such events within the limits specified by acceptance criteria. The scenarios depend on the performance of safety systems designed to mitigate the consequences of undesired events and to prevent the accident in any case. Therefore additionally, single or multiple failures of these systems are postulated during the DBA analysis. Moreover, the conservative assumptions

are made in such a study in order to demonstrate that the relevant safety functions can be provided despite the postulated failures even in the worst case [37]. To meet such strict requirements it is necessary to maintain appropriate safety margins and to implement the fundamental rules of the defence in depth (DID) methodology.

The DID approach to the design and operation of nuclear power plants aims to ensure that there are multiple safety systems and barriers, designed to prevent core damage, containment failure and consequently release of radioactive material outside the plant. Therefore, the redundancy of safety systems must be guaranteed, which means their physical separation and diversity. In other words, almost each safety system is able to play more than one role, depending on time and type of an accident, which means it can be used to perform different functions while different accident scenarios. It implies that one safety function, crucial to prevent the consequences of undesired event, can also be performed by a few separated technical installations using different equipment, which ensures the alternative way to the accident counteraction. It is also a good practice to use different physical processes in the alternative systems intended to perform concrete safety function, e.g. reactor shutdown can be achieved by both dropping control rods into the core and injecting boron into the primary coolant system. In such a case the function of a mechanical system can be taken over by the chemical one.

Another issue is the independence of safety systems, which is crucial to avoid the common cause failure of a few installations at the same time. In particular, it is important to provide redundant electrical power supply for each safety system, meaning that at least two separated external sources are needed. However, the active systems are to support the five physical barriers between the radioactive material and the environment, namely: fuel material, fuel cladding, boundary of primary loop (including reactor pressure vessel), containment and reactor building [27, 28]. Any change of the NPP configuration that could bring some benefits, but also may lead to loss any of DID barriers is not acceptable according to IRIDM.

Safety margins describe the difference between the limiting values of assigned parameters and their actual values. Since the limiting values must not be exceeded, because it would lead to failure of important structures, systems or components (SSCs), existence of appropriate margins assures safety of nuclear power plants in all modes of operation. The highest priority is given to those safety margins, that are related to physical barriers protecting against the release of radioactive material. This safety margins are commonly expressed as a maximum fuel temperature, peak clad temperature, its oxidation level, reactor coolant pressure, stress and material condition, reactor containment pressure and temperature, radiological doses to the staff and the public. However, the precise determination of safety margins for these parameters is often very hard to obtain or even impossible. It is because, in many cases, both the limiting values of the relevant parameters and their actual values are provided by the calculations with usage of complex computer codes.

Since the computer simulations provide the results with uncertainties and not the exact real values, there are two options to assess the appropriate level of safety margins. First one is based on conservatism in calculations, which means pessimistic approach during the whole process (Fig. 3). This approach is assumed to determine the safety margins much lower than they actually are, which is not optimal from the economic point of view, because it needs some additional resources to balance the very pessimistic assumptions [25]. Therefore the second solution, leading to the best estimation of safety margins, is more and more commonly applied. This approach, based on realistic assumptions instead of the pessimistic ones, is additionally supplemented by the uncertainty analysis. As a result the actual value of a particular parameter is estimated by the calculated one including the upper bound of its uncertainty.

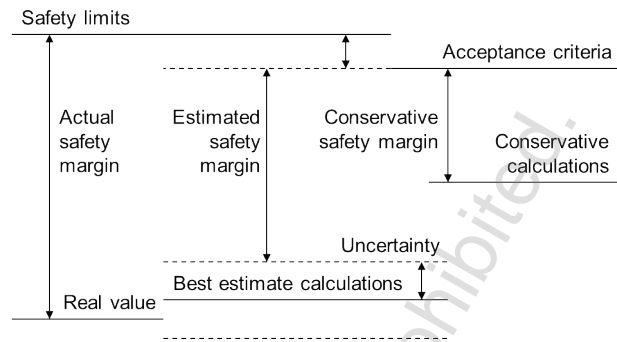


Fig. 3. Different approaches to the assessment of safety margins [cf. 25]

In both the pessimistic and best estimate approach to safety margins, the criteria established by the regulatory body are usually more restrictive than the actual limiting values, which makes the overall assessment more conservative. Regardless of the approach to assessing the safety margins, every time when IRIDM decision leads to its reduction it must be subjected to a detailed examination.

4.6. Probabilistic considerations

Probabilistic analysis is intended to complement deterministic approach by identification of all contributions to the risk in an integrated model that otherwise may be overlooked. The outcomes from these considerations include both quantitative and qualitative insights to the IRIDM process.

Probabilistic Safety Assessment (PSA) is an essential element of IRIDM because it provides relevant information on all possible initiating events, internal hazards (including fires and floods), external hazards (including seismic events), system failures and human errors, that would potentially lead to a nuclear accident. Afterwards various sequences of the accident progress can be identified depending on the success or failure of safety systems required to mitigate the consequences of undesired, but predicted events. These sequences are then depicted in a form of an event tree (Fig. 4).

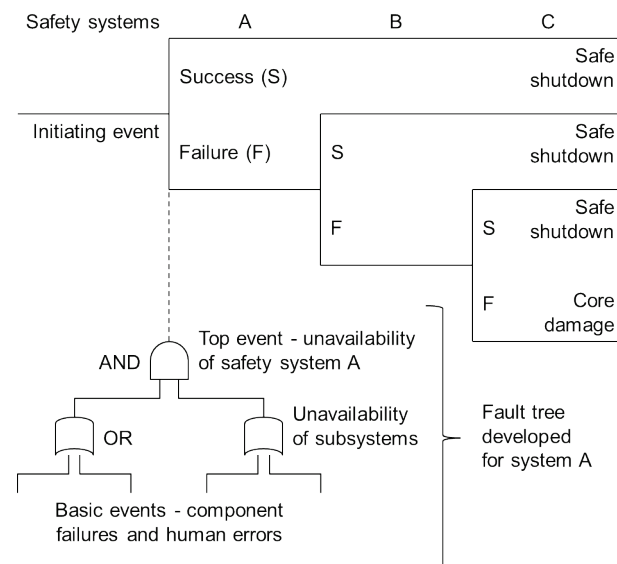


Fig. 4. Simplified diagram of PSA Level-1 – event tree and fault tree construction

Since the reliability of particular safety systems can be obtained based on probabilities of basic equipment failures and human errors, the identified accident sequences can be evaluated quantitatively as well. In order to quantify the event tree, it is necessary to develop a fault tree for each relevant safety system, by identification of basic events, i.e. equipment failures and human errors, and their relations. Moreover, the frequency of each basic event has to be assessed based on operational

experience or external database. It makes this approach capable of calculating the frequency of each accident sequence, and especially those leading to the reactor core damage.

The methodology described above is related to PSA Level-1 and aims to calculate the core damage frequency (CDF) [33]. PSA Level-2 models phenomena that could occur following the core damage, challenges to the containment integrity and transport of radioactive material in the containment. At this stage potential ways for the radioactive releases from the nuclear facility to the environment are investigated. As a result large release frequency (LRF) can be estimated in the same way as those for the core damage frequency [34]. Level-3 PSA models the consequences of such releases in order to estimate the risks to the public health and societal risks like the contamination of land or food.

Thus the adverse consequences of postulated undesired events may be described as a function of various factors like equipment failures, human errors or weather conditions. Since these factors are statistical, the technical design features and internal procedures must minimize the risk. It implies that the IRIDM decision on changing installation design or operational procedures should not significantly increase neither the CDF nor LRF. Often instead of frequencies, which describe the expected number of occurrences per year, dimensionless probabilities or conditional probabilities are used to present the PSA results.

Besides of quantitative PSA outcomes, i.e. CDF and LRF, there are also qualitatively important insights. It was recognized, that the PSA logic model itself, even without of the reliability data, is an important source of relevant information on safety issues. The main advantage of this methodology is the comprehensive approach to all facility systems, which allows to conduct analysis of the interrelations between very basic components and their impact on overall safety.

First of all, the relative impact of IRIDM decision on the facility can be observed by simple modification of the PSA model with accordance to the considered IRIDM option. Comparing PSA models for both cases, before and after modification postulated by IRIDM, it is often possible to state if the changes are qualitatively positive or negative, when it comes to the safety. For example if the proposed changes lead to reduce redundancy level of electric power supply the core damage frequency will certainly increase significantly. Additionally, based on the PSA logic model it is possible to indicate these systems, availability of which would be especially affected by the proposed changes. It is also possible to check how many different events could be potentially caused by each single failure or human error.

On the other hand so-called minimal cut sets (MCSs) can be specified as the minimal combinations of component's failures and human errors leading to undesired state of particular safety systems or the installation as a whole. The MCSs review of the probabilistic model allows to identify if there is a compliance with the single failure criterion, which is one of the fundamental design principles and aims to ensure that there are no single events leading directly to the whole system unavailability.

4.7. Organizational considerations

Organizational issues are increasingly important and need to be considered when making a decision within the IRIDM process next to the safety analyses. Typical inputs from these considerations include information related to the management systems under both normal and emergency operating conditions. In order to enhance safety the management process should cover a wide range of aspects including competence development by appropriate trainings for staff, systematic inspection of equipment maintenance and tests, taking care of good communication and cooperation between staff as well as refinement of internal procedures and many other organizational actions [36].

However, from the IRIDM point of view, it is important to identify how does the proposed option might affect an existing organizational system and how many efforts needs to be made in order to implement and monitor the decision. Finally, even if there is a formal readiness to many organizational changes, like e.g. employment increasing, specialized trainings for new staff, equipment modernization and development of additional procedures, the main question is if there is enough time and financial resources to achieve the goals. If the answer is not, the IRIDM option will be rejected, irrespective of good results from the preliminary safety studies.

4.8. Security considerations

Physical protection of the nuclear facility and the nuclear material on the site is crucial to reduce the potential threat of terrorist acts. However, since some interfaces between safety and security issues exist their proper integration in the IRIDM process is required. Therefore it is especially important to consider all security challenges related to the proposed IRIDM option in the context of their safety impact. Moreover, the security issues may be associated with new investments and structural changes, which should be also taken into account during the IRIDM process [35].

4.9. Other considerations

Although the IRIDM process has been assumed and developed as a set of concrete issues to be considered every time when non-routine decision needs to be made, its framework is not completely fixed nor limited to only those aspects, which were described above. There are also other special considerations, relevant for each particular problem, which need to be identified and included into the IRIDM framework. These additional factors could be related to workers irradiation risks during hardware modifications, economic costs and benefits of the postulated changes or the new results of scientific research.

The radiation doses, that would be received by the workers involved in the facility modification process, would need to be estimated for each of the options evaluated during the IRIDM considerations. Then the estimation results should be compared with the doses from normal operation and the difference would need to be calculated and included into the IRIDM process as an important factor. Consequently, the final IRIDM decision should ensure the minimization of the additional doses.

It is also a generally known statement that the safety measures have their economic effects, costs and benefits, that should be balanced. Although in general the safety issues are the priority and the acceptance criteria must be met in any case, some additional improvements may be blocked by insufficient financial resources. Resignation of heavy investments may be justified especially when there is a short remaining lifetime of the facility.

5. Uncertainty assessment in the IRIDM process

There is a general international agreement, that both the deterministic and probabilistic approaches, when considered together in a complementary manner, form a mature enough and comprehensive methodology of safety assessment. However their limitations should be also indicated.

In general there are two major types of the PSA uncertainties: aleatory (i.e. the inherent variability of the measurable physical quantities) and epistemic ones (coming from lack of complete knowledge about systems, processes and modelled phenomena). While the first type is irreducible, the second one (including parameter uncertainty, model uncertainty and completeness uncertainty) may be reduced over time by additional measures, testing and analyses. In this paper both aleatory and epistemic PSA uncertainties are discussed in the context of the decision making process.

The uncertainty analysis is also associated with deterministic studies and includes model simplifications, input data uncertainties and computational accuracy. Moreover there are some limitations related to availability of adequate hardware resources. All these aspects of the DSA uncertainties are discussed below in more detail.

5.1. Uncertainties of deterministic considerations

The deterministic studies, based on computer simulations, are very complex and need multidisciplinary knowledge and experience. First of all, the virtual 2D or even 3D model corresponding to the real system has to be developed. Then the whole volume occupied by the model is divided into discrete cells forming the volume mesh or nodalization. However, due to high complexity of such a geometry some general assumptions have to be made. The simplification of the system geometry implies the reduction of results accuracy at the very beginning of the analysis.

Another uncertainties come from input data. Usually the one who performs the simulation is not the one who do the measurements during the experiment. Lack of the measurement background information will certainly lead to make some assumptions when simulation setup is prepared. From time to time, some of the parameters necessary to put into the code are simply impossible to measure. This means, certain assumptions, generally conservative, have to be taken into account again. The problem is that every assumption (especially conservative one) introduces undesired uncertainty. Hence, the safety margin become blur and inexact. Also, in most of the cases the experiment is designed to prove existence of appropriate safety margins in real-life reliable conditions and not necessarily to support the DSA simulation which creates another space for speculations.

When the setup is ready to run, another source of uncertainties in deterministic analysis appears. This is a numerical calculation which always give an approximate, but never the accurate solution. Thus the physical phenomena, simulated in order to check if the safety margins are retained during the postulated accident, cannot be accurately described. The quality of results may depend on software, i.e. finite computational accuracy, introduction of empirical models, which not always fits the range of application, inaccurate implementation of methods from handbooks etc. may and surly will affect final results.

Finally, there is also an user effect issue that should be outlined. It is a quite common situation when two or more analysts are performing the same simulation, basing on the same input data, using the same software, but achieving different results. This is due to their experience, routine, perceptivity and so on.

Moreover, the more complex geometry needs to be mapped in details, the lower scale of mesh elements is required, which leads to increase of the computational domain. It is because the appropriate calculations are performed for each element in the volume mesh of a higher density. It provides the higher resolution of the results, but also the high performance computing is needed, which implies additional limitations related to computation time and availability of hardware resources.

5.2. Uncertainties of probabilistic considerations

The uncertainty analysis is even more integrated with the probabilistic approach. It is because its methodology is used in modelling of processes and phenomena, that can be described only statistically. Consequently, the initiating events, system failures and human errors, considered by the PSA studies, have a random nature and appropriate frequencies or probabilities of their occurrence have to be assessed.

Besides of the quantitative assessment, the PSA analysis itself bases on the development of event trees and fault trees linking the events through the logical gates (Fig. 4). Thus the uncertainties corresponding to the particular basic events can propagate in the whole logical structure influencing the top events

probabilities. Consequently, both these elements, development of the PSA logic models and assessment of basic events frequencies, introduce some uncertainties, which could have a significant impact on the final PSA results [40].

Since the PSA uncertainties have different sources, there are also different types of them, aleatory and epistemic, which should be analysed separately. The first one is associated with the inherent variability of measurable physical quantities, which implies the random nature of the initiating events and component failures. Thus the aleatory uncertainties cannot be reduced neither by further studies nor even by enlarging of the data set, but they can be assessed based on the traditional data analysis.

Database enlarging can, however, improve the representation of the probability distribution of those stochastic variables, like time to failure or time to repair, for all components of the system. Then the Monte Carlo method can be used in order to assess the aleatory uncertainty as well as the mean value and variance of the top event probability. It can be accomplished by sampling of the probability density functions of stochastic variables corresponding to the particular failures [10].

The epistemic uncertainties arise when making statistical inferences from the data, due to a lack of complete knowledge about systems, processes and modelled phenomena. In contrast to the aleatory uncertainties, the epistemic ones may be reduced over time, by additional measures, testing and analyses, leading to increase the data set and the knowledge. There are three types of epistemic uncertainties in PSA: parameter uncertainty, model uncertainty and completeness uncertainty. The identification, understanding and consideration of these types of uncertainties is crucial for the comprehensiveness of PSA study and consequently for the IRIDM process [16].

Parameter uncertainties relate to the computation of the input parameter values, used to quantify probabilities of the events in the PSA logic model, given that the mathematical form of the model itself has been agreed to be appropriate. It is a common practice to characterize these parameters by using probability distributions instead of their point values. Thus the treatment of both aleatory and parameter uncertainties, requires a two-loops Monte Carlo simulation. The outer loop samples the epistemic variables, when the inner loop is to aleatory ones [8, 13]. In addition, the epistemic correlations, when the same parameter is used to quantify the probabilities of two or more basic events, should be considered. Otherwise, if the correlation between the events is neglected, the uncertainty of system failure probability would be underestimated [40].

Model uncertainties are related to such cases, for which no consensus approach or model exists. Thus, if the chosen model is not suitable to represent a particular aspect of the plant, the uncertainty of PSA results would also exist. It comes from a lack of knowledge of how the SSCs can behave under the conditions arising from an accident. It is because some of the phenomena being modelled are not completely understood yet. Moreover, for some of them, the existed data or other information were collected under different conditions than those expected during the postulated accident. Therefore the model uncertainties assessment usually needs the expert judgment [4].

Another issue is the completeness uncertainty. It represents those aspects that are, either knowingly or unknowingly, not addressed in the model. The omission of some aspects can result from the lack of suitable methodology for the analysis of them. The resources to develop a complete model may be also limited, which implies simplifications.

6. The general concept of the integration process

The main challenge of the IRIDM process is to indicate the best option solving the specified issue in a logical, structured, and comprehensive manner. This approach leads to transparency of the decision making process and allows to understand why and how the decision was reached, which factors were taken into account and what was their relative importance. The decision

made in that way, when documented sufficiently, is reproducible and can be verified by independent group of specialists [36].

In order to achieve an optimal and unbiased solution of the postulated issue, the appropriate integration of different IRIDM elements is needed. First of all, it must be demonstrated that the essential requirements are satisfied for each element separately. For that purpose an implementation of some additional safety measures could be required, but these improvements must not affect adversely the other IRIDM inputs.

However, since all key elements of IRIDM are somehow depended on each other, the integration process should be an iterative one and consideration should be given to all inputs again after one of them has been changed. If the proposed improvements leading to meet one of the safety factors adversely affect at least one another, one needs to consider an implementation of alternative safety measures to ensure the acceptability of all relevant factors.

Figure 5 depicts the combination of the deterministic and probabilistic elements, which is a part of the overall IRIDM integration process. The deterministic considerations answer question if the safety systems are able to meet their design intent properly and if the other requirements like defence in depth or safety margins are ensured. The PSA instead investigates all possible sources of equipment failures, human errors, internal and external hazards, which could lead to unavailability of safety systems or breach of the safety barriers.

There are also some interfaces between these two elements. It is enough to mention that deterministic calculations are used to specified the success criteria for each safety system, that are required as an input to the PSA analysis. These success criteria mean the minimum conditions, under which the designed safety system is recognized to be sufficient to perform its functions properly, even if there are some failures of its single components. Basing on that criteria, the total system unavailability or severely limitation of its functionality can be defined, which is crucial for system reliability assessment under accident conditions.

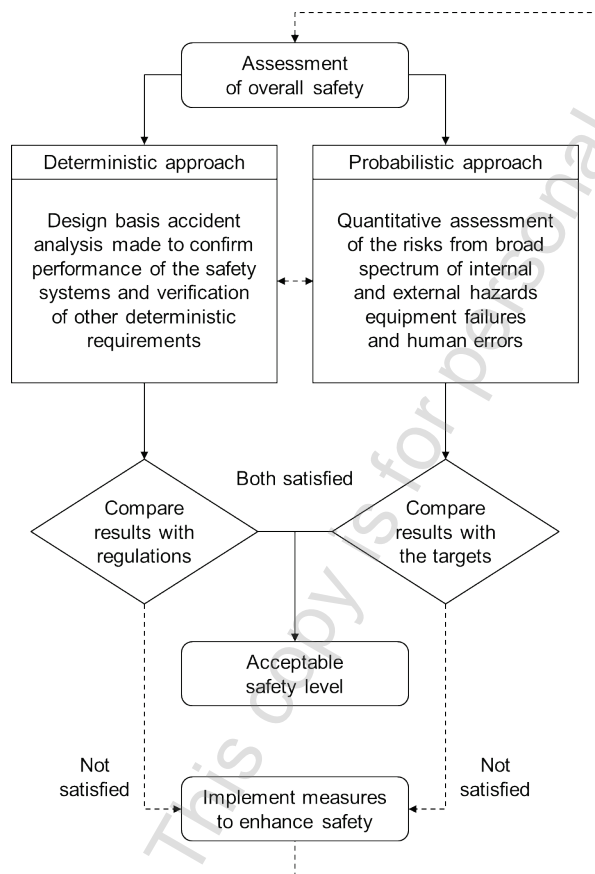


Fig. 5. Integration of deterministic approach and probabilistic insights [cf. 36]

On the other hand, the probabilistic considerations are able to indicate additional initiating events, which should be included into the deterministic studies. Moreover, the PSA methodology is used in prioritising of the events in order to focus more intensively on those cases that are more probable. It is also applicable to define assumptions for the so-called risk informed best estimate deterministic calculations, which are more and more commonly applied instead of conservative ones. The deterministic results are then compared with appropriate acceptance criteria given by the regulatory body, while the PSA insights are assessed in the context of risk minimization. Only when the requirements of both are satisfied the IRIDM option can be implemented.

Nevertheless, the major challenge of the integration process is to assess the relative importance of various qualitative and quantitative inputs in the single IRIDM implementation, as it will be described later in this paper.

7. IRIDM implementation and workflow process

The general framework of the IRIDM process, described in this paper, can be applied to decision making by all stakeholders involved in the nuclear industry, i.e. the regulatory bodies, NPP operators and technology vendors. However, some necessary prerequisites have to be met before implementing the IRIDM approach to consider a certain issue.

7.1. Preparation for performing IRIDM

Prerequisites of the IRIDM implementation may be developed as a consensus between the stakeholders (Fig. 6). Through the cooperation of the regulatory body, NPP operator and TSO, the risk informed safety policy needs to be established at the national level. While the ultimate responsibility for the policy lies as usually in the competence of the regulatory body, the cooperation between stakeholders has been recognized as an important aspect of the preparation process for the IRIDM performance.

The safety policy, prepared in that way, should cover the high level safety goals and acceptance criteria to be applicable in the future implementations of IRIDM [11]. It may also indicate possible ways to exempt from the specified regulatory requirements or even to changing them in very special cases, if these requirements are against the justified proposals or conclusions of IRIDM.

Once the national policy is approved the decision to apply IRIDM approach in the future activity of the stockholders can be taken. However the potential limitations of the IRIDM process in the specific organization has to be analyzed.

The major factors influencing the implementation of the IRIDM methods within the specified organizational structure are the following: relevant infrastructure, competence base and computational codes. Therefore the existing organizational structure, employees competencies, computational resources as well as the management system itself should be adjusted to carrying out the formal IRIDM process regularly before its first implementation.

Since the organizational changes, mentioned above, may cause many complex issues, the detailed IRIDM implementation programme needs to be developed within the organization in order to resolve them all in the structured manner. The programme for the IRIDM implementation should indicate the potential fields of its applicability first. It means that the range of issues should be defined by the regulatory body and shared between stakeholders. Then one needs to provide and develop the whole infrastructure suitable to perform and review the analyses covering the specified IRIDM inputs. This infrastructure then should be capable to understand the conclusions from that process. It requires the identification of the expertise areas to be covered and the assessment tools to be provided.

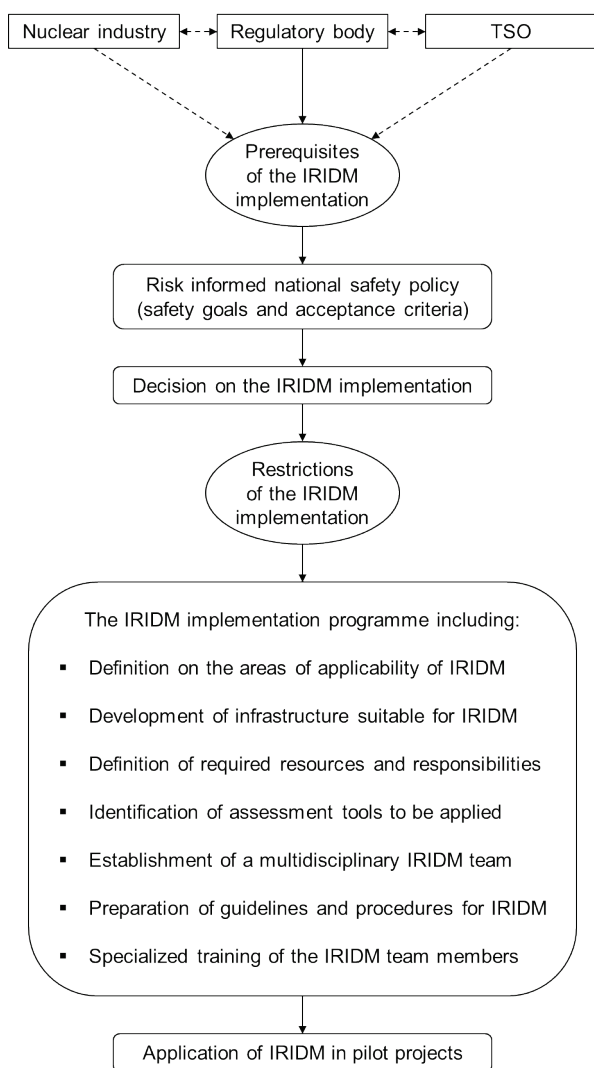


Fig. 6. Initial preparations for the IRIDM process implementation [cf. 11]

Another important issue is the division of responsibilities regarding IRIDM between individuals within the organization. It is a common practice in the industries, where various risks for the public exist, to train a group of leaders responsible for different types of them. Moreover, there are also specialists for financial risk assessment, responsible for minimization of the financial losses or bankruptcy probability. Thus, the risks associated with the industry should be interpreted not only in terms of the potential hazards, which poses some threats to the environment or to the public, but also in the context of decrease in production efficiency or financial losses, leading to the suspension or even cessation of the activity. This is the reason why the risk informed decision making process in the industry as a whole should be an integrated one.

The same approach is applicable in the nuclear industry through the explicit IRIDM implementation. First, the special IRIDM team needs to be established within the organization. Since the IRIDM process covers a wide range of issues, from technical, through economic up to the psychological ones, it is essential for the team to be multidisciplinary, which means its members should be specialists in their fields. Then the leaders, responsible for different IRIDM inputs, corresponding to various risks, should be selected from the team members. The leaders, however, are expected to be interdisciplinary, which means capable to understand and evaluate the significance of conclusions coming from different inputs, in the light of that type of risk, which has been assigned to them.

To fulfil its mission, the team needs to be intensively trained for implementing the IRIDM methodology into the real problems. However, while the understanding of the IRIDM principles is relatively simple, their practical application is usually very

difficult. Therefore, besides of the general IRIDM training for the team as a whole, some specialised courses on various fields are necessary to be provided systematically for each group, according to its activity area within the team.

Moreover, the knowledge gained from the trainings and from experience as well should be documented in a form of guidelines describing the best practices for the IRIDM implementation. On that basis some internal procedures and tools can be developed for the teamwork improvement. After that it is recommended to carry out the pilot project in order to test the IRIDM methodology, review the team capability and verify the guidance and procedures in a realistic, but small scale preliminary study.

7.2. Implementation of the IRIDM process

Practical application of the IRIDM process requires a number of systematic steps and activities to be performed in a logical order according to the overall workflow (Fig. 7).

The first stage, covering characterisation of the issue, drafting the initial set of options and formation of the IRIDM team, has been described above. However, it should be mentioned here, that for specific issues the permanent IRIDM team may be expanded by additional, even external, experts in order to provide required technical support or specialized consultations.

The second step of the IRIDM workflow is the analysis of its feasibility for the specified problem to be solved. It aims to identify all potential obstacles associated with the specific issue under consideration. It includes the complexity of the problem, period of the time required for IRIDM performance in the context of deadlines and terms imposed by the regulatory body, as well as the availability of financial resources for the comprehensive studies. Thus the IRIDM implementation may be abandoned because of lack of specialists, lack or incompleteness of information regarding the IRIDM inputs, high uncertainties of the analysis methods applied in specified area or lack of appropriate software tools. In such a case one needs to try another method to solve the issue, the less expensive or less time-consuming one, keeping in mind that it also means less comprehensive than the IRIDM is.

However the answer to the question, if the IRIDM process is feasible for the specific issue, is not always simple yes or not. Usually, only some options selected from the initial set of solutions to be considered are rejected at this stage, while the others can be analyzed in the next stages of IRIDM.

After the decision has been made to implement the formal IRIDM approach into the specific issue, one needs to start initial preparations for the assessment of the identified inputs required by the decision making process. It is important to ensure the following things: completeness of detailed technical information, sufficient quality of the data with specified uncertainties as well as appropriate validation of analytical tools and models used in the IRIDM process. All inputs should be evaluated for all decision options to check whether the proposed solutions meet the existing acceptance criteria. Furthermore, it is a good practice to provide an independent review of once made analysis in order to verify the results credibility.

The next stage of the IRIDM implementation is the integration process. It aims to determine the weights to be attributed to each of the inputs in the IRIDM process. However, the weighting scale for the inputs needs to be established first. The weighting scale describes the range of values for weighting factors assigned for particular types of risk. In practise there are two general ways for the factors assessment. Qualitative or quantitative approach can be applied to achieve it. The first one is to divide the inputs into three categories according to their significance for the considered issue: high, medium and low. The alternative way is to assign them the numerical values from 0 – negligible impact, up to 10 – the highest impact on the decision. During the weighting process one needs to remember that the factors are to specify the relative importance of each input in relation to the others [11]. Moreover the weights assigning is quite

subjective, based on the engineering judgment and dependent on the particular issue being addressed. Therefore various techniques have been developed in order to improve this process so that it can be carried out in a clear, understandable and reasonable manner [1, 7, 17].

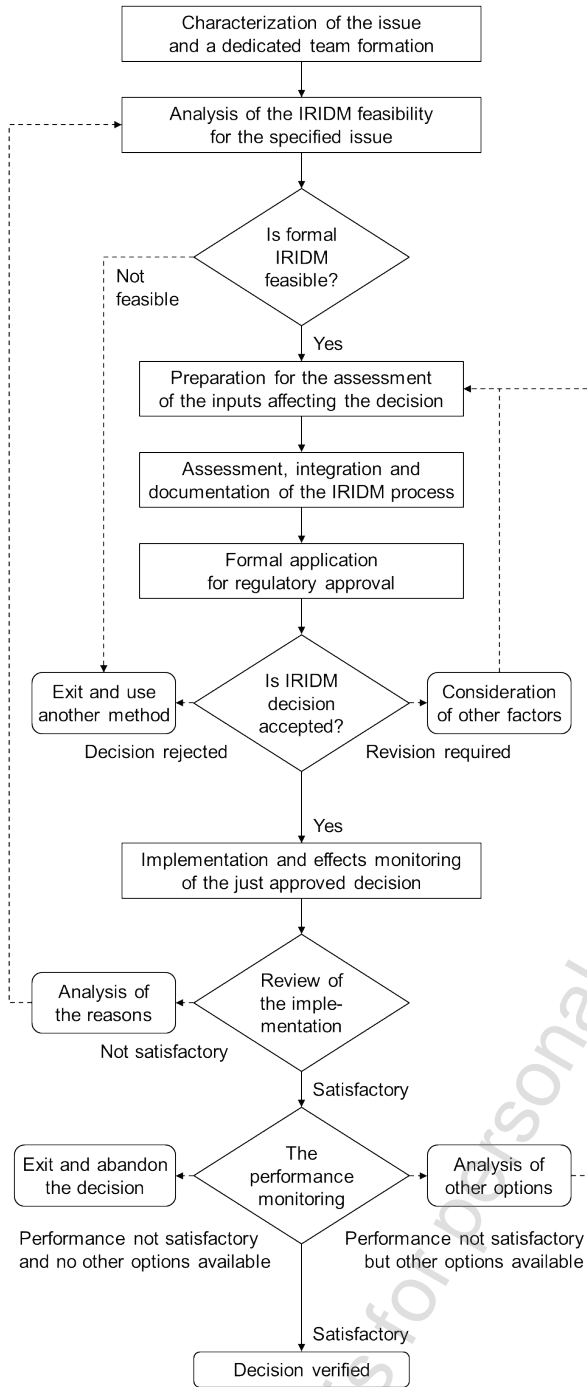


Fig. 7. The overall workflow of activities in the IRIDM process [cf. 37]

As a result of the weighting process the inputs can be ranked by their relative significance for the considered issue. Then one can determine the impact of the various IRIDM options on the particular inputs. Usually at the beginning the qualitative impact assessment is performed. It means each option needs to be analyzed in the context whether it has a positive or negative impact on each particular input. After that the score can be assigned for each option in the range of values from -10 (the highest negative impact) through 0 (no impact) up to 10 (the highest positive impact). It allows to evaluate the option i by the total weighted score (S_i) described by the equation below:

$$S_i = \sum_j w_j \cdot s_{ij}, \quad (3)$$

where w_j is the weighting factor of the input j and s_{ij} is the impact of option i on the input j based on the scoring approach. Consequently, all initially proposed options can be ranked by that factor and the best solution can be selected. The recommendation is given for that option which has the highest positive impact or, if all are negative, the lowest one.

Having selected an option, final documentation of the IRIDM process and its results should be prepared. This documentation is essential for the IRIDM implementation while making it traceable and reproducible. On this basis, formal application for approval of the selected solution can be addressed to the regulatory body, which has the necessary authority to its acceptance, rejection or to request additional revisions.

Since IRIDM is an iterative process, the implementation of the decision should be reviewed and its performance needs to be monitored. If the real implementation is found to be different than described in the documentation, the potential reasons should be analyzed. In such a case one needs to go back into the feasibility stage. On the other hand, if the performance of well-implemented option is not satisfactory, the other one should be considered.

7.3. Risk informed regulation

Although the IRIDM approach has been developed to be applied in making decisions on safety issues of nuclear facilities, it may be also useful to specify the way in which a regulatory body should carry out its activities.

As an example the risk informed process of the national regulations improvement can be considered with accordance to the diagram depicted in the figure 8. First, the existing regulations should be reviewed in the terms of possible changes potentially leading to the safety improvement. As a result the list of requirements, that are candidates to be modified, can be developed. From that list those elements, for which the risk informed approach is suitable, should be identified and prioritized according to a number of factors including the risk information. It means the regulatory body can weigh these factors and make a judgment on priorities of the proposed changes based on their impact for safety as well as time and resources needed for their full implementation. Different options for modification of particular requirement can be also considered and scored.

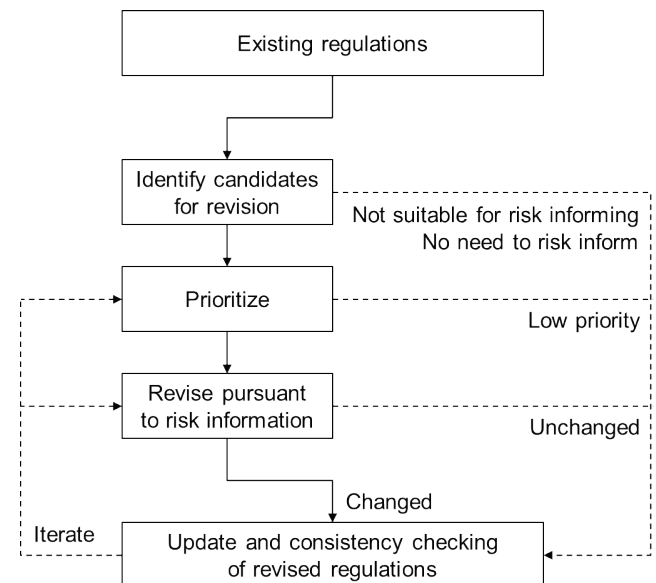


Fig. 8. Risk informed process of improvement the national regulations [cf. 29]

The last step aims to verify whether the approved modification of specific requirement is not in contrary to the other regulations. Since this is the iterative process one can back to the previous steps and select another regulations to be checked for possible improvements.

8. Conclusions

Making a complex decision should always be a structured process, not just an act, especially when it comes to the public safety. In the nuclear industry an integrated approach to the risk informed decision making (IRIDM) is being promoted by such organizations as the International Atomic Energy Agency and the United States Nuclear Regulatory Commission (U.S. NRC).

In this article the fundamentals of the IRIDM process have been thoroughly described based on both the IAEA documentation and the U.S. NRC reports. Major benefits of complementary approach to the deterministic and probabilistic considerations have been specified here as well.

First of all, the PSA analysis is possible to determine whether any group of initiating events makes a contribution to the risk that is much higher than the others. It implicates greater levels of redundancy and diversity of that equipment, which is intended to prevent the most probable events.

Comprehensiveness of PSA is another advantage of such kind of studies. Since all initiating events and SSCs are included in a single model, it is possible to derive the relative importance of each of them explicitly and, what is sometimes even more important, their interrelations. The same applies to the interdependencies between the various levels of defence in depth implementation.

Although the IRIDM is widely regarded as a transparent, balanced, logical and consistent process, the limitations of this approach have been also indicated here.

9. The IAEA Safety Glossary

The IAEA Safety Glossary [30] is used to define and explain technical terms used in the paper:

Acceptance criteria – Specified bounds on the value of an indicator – characteristic of a structure, system or component that can be observed, measured or trended – used to assess the ability of a structure, system or component to perform its design function.

Availability – the fraction of time for which a system is capable of fulfilling its intended purpose.

Common cause failure (CCF) – failure of two or more structures, systems and components due to a single specific event or cause.

Defence in depth (DID) – A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

Design basis accident (DBA) – Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

Licensing process – the authorization process leading to the grant of a licence, which is a legal document issued by the regulatory body granting authorization to perform specified activities related to a facility or activity.

Multiple barriers – Two or more natural or engineered barriers – physical obstacles that prevent or inhibit the movement of people, radionuclides or some other phenomenon, or provide shielding against radiation – used to isolate radioactive waste in, and prevent migration of radionuclides from, a repository.

Nuclear safety – The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards.

Nuclear security – The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Operator – Any organization or person applying for authorization or authorized and/or responsible for nuclear, radiation, radioactive waste or transport safety when undertaking activities or in relation to any nuclear facilities or sources of ionizing radiation. This includes, inter alia, private individuals, governmental bodies, consignors or carriers, licensees, hospitals, self-employed persons.

Radioactive waste – For legal and regulatory purposes, waste that contains, or is contaminated with, radionuclides at concentrations or activities greater than clearance levels as established by the regulatory body.

Reliability – probability that a system or component will meet its minimum performance requirements when called upon to do so.

Research reactor – A nuclear reactor used mainly for the generation and utilization of neutron flux and ionizing radiation for research and other purposes, including experimental facilities associated with the reactor and storage, handling and treatment facilities for radioactive materials on the same site that are directly related to safe operation of the research reactor. Facilities commonly known as critical assemblies are included.

Safety analysis – Evaluation of the potential hazards associated with the conduct of an activity.

Safety assessment – Assessment of all aspects of a practice that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility.

Safety function – A specific purpose that must be accomplished for safety.

Safety system – A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

Sensitivity analysis – A quantitative examination of how the behaviour of a system varies with change, usually in the values of the governing parameters.

Single failure criterion – A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

Structures, systems and components (SSCs) – A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors.

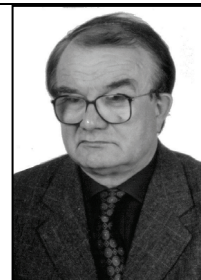
Acknowledgements

The authors of this paper are pleased to acknowledge the participants of the Regional Workshop on Advances and Issues in Integrated RIDM, organized by the International Atomic Energy Agency (IAEA) in collaboration with the Bulgarian Nuclear Regulatory Agency (BNRA), held in May 2012, in Sofia (Bulgaria). The presented work was supported by the EU and MSHE grant nr POIG.02.03.00-00-013/09.

References

- [1] Ahn B.S., Park K.S.: Comparing methods for multi-attribute decision making with ordinal weights. *Computers and Operations Research* 35/2008, pp. 1660-1670.
- [2] Borysiewicz M., Furtek A., Potemski S.: Poradnik metod ocen ryzyka związanego z niebezpiecznymi instalacjami procesowymi. Instytut Energii Atomowej, Otwock-Swierk 2000.
- [3] Borysiewicz M., Kowal K., Potemski S.: Decision making for safety of technological installations based on risk. *Proceedings of the XIX Scientific-Technical Seminar of Materials Investigation for Power Industry, Zakopane 2012*, pp. 209-219.
- [4] Cooke R.M.: *Experts in Uncertainty. Opinion and Subjective Probability in Science.* Oxford University Press, Oxford 1991.
- [5] Govaerts P.: Roles, functions and value of TSOs. *Proceedings of an International Conference on Challenges Faced by Technical and Scientific Support Organizations in Enhancing Nuclear Safety, Aix-en-Provence 2007*, pp. 49-54.
- [6] Hahn L.: Independent technical and scientific advice for regulatory decision making. *Proceedings of an International Conference on Challenges Faced by Technical and Scientific Support Organizations in Enhancing Nuclear Safety, Aix-en-Provence 2007*, pp. 55-65.
- [7] Jia J., Fisher G.W., Dyer J.S.: Attribute weighting methods and decision quality in the presence of response error: A simulation study. *Journal of Behavioral Decision Making* 11/1998, pp. 85-105.
- [8] Knudsen J.K., Smith C.L.: Estimation of system failure probability uncertainty including model success criteria. *Proceedings of the 6th International Conference on PSA and Management, San Juan 2002*, pp. 201-206.
- [9] Ko K.S., Han K.I.: Relevance of TSOs in providing technical and scientific services to operators/industry. *Proceedings of an International Conference on Challenges Faced by Technical and Scientific Support Organizations in Enhancing Nuclear Safety, Aix-en-Provence 2007*, pp. 67-85.
- [10] Lee J.C., McCormick N.J.: *Risk and Safety Analysis of Nuclear Systems.* John Wiley & Sons Inc., Hoboken 2011.
- [11] Lyubarskiy A., Kuzmina I., El-Shanawany M.: Advances in Risk Informed Decision Making – IAEA's Approach. *Proceedings of the Nordic PSA Conference, Gottröra 2011*, pp. 1-14.
- [12] Małecko L.: Introduction to the nuclear energy in Poland. *Proceedings of the XIX Scientific-Technical Seminar of Materials Investigation for Power Industry, Zakopane 2012*, pp. 1-40.
- [13] Rao K.D., Kushwaha H.S., Verma A.K., Srividya A.: Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. *Reliability Engineering & System Safety* 92/2009, pp. 947-956.
- [14] Strupczewski A.: Safety classification of nuclear power plants structures, systems and components and their qualification. *Proceedings of the XIX Scientific-Technical Seminar of Materials Investigation for Power Industry, Zakopane 2012*, pp. 57-84.
- [15] Valtonen K., Vantola T.: Role of the TSO in public information/debate openness, transparency. *Proceedings of an International Conference on Challenges Faced by Technical and Scientific Support Organizations in Enhancing Nuclear Safety, Aix-en-Provence 2007*, pp. 97-102.
- [16] Volkanovski A., Čepin M.: Implication of PSA uncertainties on risk-informed decision making. *Nuclear Engineering and Design* 241/2011, pp. 1108-1113.
- [17] Xuan S.: A Novel Kind of Decision of Weight of Multi-attribute Decision-Making Model Based on Bayesian Networks. *International Seminar on Business and Information Management 2/2008*, pp. 30-33.
- [18] Health and Safety Executive: *The tolerability of risk from nuclear power stations.* HSE Books, Sudbury 1992.
- [19] Health and Safety Executive: *Reducing Risks, Protecting People: HSE's decision-making process.* HSE Books, Norwich 2001.
- [20] International Atomic Energy Agency: *Equipment qualification in operational nuclear power plants: upgrading, preserving and reviewing.* IAEA, Vienna 1998.
- [21] International Atomic Energy Agency: *Basic safety principles for nuclear power plants.* IAEA, Vienna 1999.
- [22] International Atomic Energy Agency: *Quality assurance within regulatory bodies.* IAEA, Vienna 1999.
- [23] International Atomic Energy Agency: *Operational safety performance indicators for Nuclear Power Plants.* IAEA, Vienna 2000.
- [24] International Atomic Energy Agency: *Training the staff of the regulatory body for nuclear facilities: A competency framework.* IAEA, Vienna 2001.
- [25] International Atomic Energy Agency: *Safety Margins of Operating Reactors.* IAEA, Vienna 2003.
- [26] International Atomic Energy Agency: *Precursor analyses – The use of deterministic and PSA based methods in the event investigation process at nuclear power plants.* IAEA, Vienna 2004.
- [27] International Atomic Energy Agency: *Assessment of Defence in Depth for Nuclear Power Plants.* IAEA, Vienna 2005.
- [28] International Atomic Energy Agency: *Defence in Depth in Nuclear Safety.* IAEA, Vienna 2005.
- [29] International Atomic Energy Agency: *Risk informed regulation of nuclear facilities: Overview of the current status.* IAEA, Vienna 2005.
- [30] International Atomic Energy Agency: *IAEA Safety Glossary – Terminology Used In Nuclear Safety And Radiation Protection.* IAEA, Vienna 2007.
- [31] International Atomic Energy Agency: *Deterministic Safety Analysis for Nuclear Power Plants.* IAEA, Vienna 2009.
- [32] International Atomic Energy Agency: *Safety assessment for facilities and activities.* IAEA, Vienna 2009.
- [33] International Atomic Energy Agency: *Development and Application of Level-1 PSA.* IAEA, Vienna 2010.
- [34] International Atomic Energy Agency: *Development and Application of Level-2 PSA.* IAEA, Vienna 2010.
- [35] International Atomic Energy Agency: *The Interface Between Safety and Security at Nuclear Power Plants.* IAEA, Vienna 2010.
- [36] International Atomic Energy Agency: *A Framework for an Integrated Risk Informed Decision Making Process.* IAEA, Vienna 2011.
- [37] International Atomic Energy Agency: *Safety of Nuclear Power Plants: Design.* IAEA, Vienna 2012.
- [38] U.S. Nuclear Regulatory Commission: *Reactor Safety Study - An assessment of accident risks in U. S. commercial nuclear power plants.* U.S. NRC, Washington D. C. 1975.
- [39] United States Nuclear Regulatory Commission: *Safety goals for nuclear power plants operations.* USNRC, Washington 1996.
- [40] United States Nuclear Regulatory Commission: *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making.* US NRC, Washington 2009.

Ph.D. Mieczysław Józef Borysiewicz
e-mail: manhaz@cyf.gov.pl



Deputy Head - Nuclear Energy Division at the NCBJ in Swierk. Till 2012 Director of the RU Centre of Excellence MANHAZ – Management of Health and Environmental Hazards. Visiting professor of Università di Bologna, Italy (1977, 1978, 1980, 1983) and researcher of Université Libre de Bruxelles (1972-1973). Numerous publications and monographs on major accident risk assessment and management of nuclear and chemical installations and computer aided decision support systems for NCBR emergencies.

M.Sc., Eng Karol Kowal
e-mail: karol.kowal@ncbj.gov.pl



Graduated from the AGH Univ. of Science and Tech. in Cracow in the field of Nuclear Physics. Completed postgraduate studies of Computer Science at the Rzeszow Univ. of Tech. as well as High Performance, Parallel and Distributed Computing courses at Maria Curie-Skłodowska Univ. in Lublin. Ph.D. student at the Lublin Univ. of Tech. in the field of Electrical Engineering. Participant of the IAEA workshops on the PSA and IRIDM held in Vienna (Austria), Sofia (Bulgaria), Petten (Netherlands) and Trieste (Italy).

M.Sc., Eng Piotr Andrzej Prusiński
e-mail: piotr.prusinski@ncbj.gov.pl



Graduated from Warsaw University of Technology (Poland) in the field of Nuclear Power Engineering. 1 year scholarship at Royal Institute of Technology (Sweden) funded by the Polska Grupa Energetyczna S.A. 6 weeks scholarship at CEA Grenoble (France) funded by the French Government. Currently employed as Senior Specialist at National Centre for Nuclear Research (Poland). Particular interest in combining deterministic (DSA) and probabilistic (PSA) approaches to reactor safety studies.

M.Sc., Eng Marcin Dąbrowski
e-mail: marcin.dabrowski@paa.gov.pl



Graduated from Warsaw University of Technology (Poland) at the Faculty of Power and Aeronautical Engineering in the Nuclear Power Engineering field. 1 year scholarship at Royal Institute of Technology (Sweden) awarded by Polska Grupa Energetyczna S.A. Since 2010, Specialist and Nuclear Safety Inspector at National Atomic Energy Agency (Poland) in Nuclear Safety Department. Participant of the Regional Workshop on Advances and Issues in IRIDM, organized by IAEA in Sofia (Bulgaria).

Artykuł recenzowany