The principle of Defence-in-Depth in the perspective of Probabilistic Safety Analyses in the wake of Fukushima

J. Vitázková[1] & E. Cazzoli[2]
[1]*Vitázková-Vitty, Slovakia*
[2]*Cazzoli Consulting, Switzerland*

Abstract

The principle of the Defence-in-Depth concept has been set forth by the IAEA as fundamental for the safety of Nuclear Power Plants in INSAG10 (1996). Within the time, essentially after severe accidents in Three Mile Island and Chernobyl, the concept evolved and the currently accepted definition is based on five successive layers of safety and four physical safety barriers, including organizational and administrative measures. Safety demonstrations are required to show that the safety layers and barriers provide sufficient margin to prevention or mitigation of releases of radioactivity to the environment. These safety demonstrations are well established for Design Basis Accidents. Probabilistic Safety Assessments (PSAs) assumed to be risks assessment tools also for Severe Accidents, however, enter the description of the Defence-in-Depth concept only as an afterthought and their role is marginalized to "improvement of defence in depth" and "optimization of efforts to implement defence in depth". This article investigates aspects related to implementation of defence in depth in the wake of the Fukushima accidents and in view of the historical evidence of nuclear power plants' risks considering also risk targets complying with IAEA safety objectives and principles. Analysis of the levels of currently accepted defence in depth is performed focusing on real accidents vs. PSA analyses results with objective to answer the question, if some of current defence-in-depth levels may not actually be yet a reason of concern instead of prevention or mitigation of risk, and, what should be the role of risk targets and risk assessment within the defence in depth concept.

Keywords: risk, risk target, Defence-in-Depth, Fukushima, severe accident, real accident, administrative measure, safety barrier, safety level, safety margin.

WIT Transactions on Information and Communication Technologies, Vol 47, © 2014 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK140041

1 Introduction

The terms safety, radiation protection, PSA, risk, severe accident management and Defence-in-Depth are strongly correlated and should be always perceived in connection. It is stated in Safety Principle 61 and 62 from (INSAG3 [1]), that PSA guides design and operation by identifying potential accident sequences that contribute to risk". Safety involves the prevention or reduction of potential exposure and other risks (for the minimization of danger). Radiation protection involves the prevention or reduction of radiation exposure (for the protection of health). Safety is thus primarily concerned with maintaining control over sources, whereas radiation protection is primarily concerned with controlling exposure to radiation, whatever the source, to mitigate its effects. (IAEA [2]) Defence-in-Depth (DiD) is a comprehensive approach to ensure with high confidence that the public and the environment are protected from any hazards posed by the use of nuclear power for the generation of electricity. When properly applied, DiD ensures that no single human error or equipment failure at one level of defence, nor even a combination of failures at more than one level of defence, propagates to jeopardize DiD at the subsequent level or leads to harm to the public or the environment. (IAEA [3]) The strategy of DiD is twofold: *first*, *to prevent* accidents and second, if prevention fails, *to limit* the potential consequences of accidents and to prevent their evolution to more serious conditions.

2 Defence-in-Depth concept

2.1 Historical background, lessons learned from real severe accidents

From what is said above, DiD is supposed to be the corner stone of nuclear safety but we should be aware as well, that DiD like everything else is the subject of evolution. The Fukushima accident must be perceived in the perspective that it is the last one in the chain of already occurred severe nuclear accidents, and by the term "severe" in context of this paper we address only those accidents that underwent core melt of larger extent than 25%. Thus the first accident addressed here was in 1977 in A1-Bohunice NPP, Slovakia – one small unit (less than 300 MWe) with HWGCR reactor KS150 with reported 25% core melt; the second in 1979 at Three Mile Island 2, USA – one average unit (less than 1000 MWe) PWR with 50% core melt; the third, in 1986 in Chernobyl, Ukraine – one large (more than 1000 MWe) RBMK unit with total core melt and destruction of facility; the fourth in 2011 in Fukushima, Japan – three average/large units with extensive core melt and total destruction of the facilities, plus one unit damage with risks to fuel pool. After the first two accidents no large releases or health effects were officially reported unlike the last two, which are associated with large releases into the air with never experienced environmental contamination into the ocean in the case of the accident(s) at Fukushima, which in fact is still in progress after three years from the accident. Hence, reality shows that severe accidents with large consequences happen and

they are neither bound to certain types of design nor country or safety culture typical of a country. The real consequences are of much greater significance and seriousness than forecasted by PSAs (Chernobyl accident [4–11]) because phenomena like partial or total core damage well beyond 24 hours, total destruction of containments and reactor buildings and all systems they house, common cause of more units/cliff edge effects, combination of initiating events etc. have never been considered in PSAs (see the results of the EU stress tests), or, if considered, they have been marginalized because the frequency was assessed to be too low.

Originally the concept of DiD included three levels (INSAG-10 [12]). Later, the concept of DiD was further refined to include consideration of phenomena observed during severe accidents in Chernobyl and Three Mile Island and in summary, the historical development of the concept of DiD led to a general structure of four physical barriers and five successive levels, which were described in (INSAG-10 [12]). Therefore, it should be expected, that also after Fukushima accident the DiD concept be re-evaluated with respect to all lessons learned, having in mind not only the Fukushima accident.

2.2 Currently accepted defence in depth concept

DiD comprises of 4 physical safety barriers and 5 safety layers (INSAG-10 [12]):

1st layer: Prevention of abnormal operation and failures
Means: conservative design
Barriers: fuel matrix, fuel cladding, primary circuit loop

2nd layer: Control of abnormal operation and detection of failures
Means: control, limiting and protection systems and other surveillance features

3rd layer: Control of accidents within the design basis
Means: engineered safety features and accident procedures

4th layer: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents
Means: complementary measures
Barriers: containment

5th layer: Mitigation of radiological consequences of significant releases of radioactive materials
Means: offsite emergency response

Consideration of beyond design basis accidents at nuclear power plants is an essential component of the DiD approach used to assure nuclear safety (IAEA SF-1 [13], INSAG-10 [12] and INSAG-12 [1]) even though their probability is low. Nevertheless, it should be noted here that none of the current designs of operating plants considers beyond design basis or severe accidents.

The need of re-evaluation of DiD was established in one of the recently issued documents (SNETP [14]) as challenges from the lessons learned from Fukushima: “To enhance further Defence-in-Depth capabilities for any type of initiating events, especially for severe natural hazards and any their combinations. It should be considered for existing reactors, future Gen III

reactors a well as for the development of Gen IV reactors. To address more systematically at the design stage the plant features for coping the design extension conditions (beyond design basis accidents) to assure the robustness of the Defence-in-Depth and to avoid cliff edge effects. The approach should include situations where several units on the same site are affected by a beyond design basis event."

3 Analysis of currently existing Defence-in-Depth concept

In the analysis we try to follow the major postulate in this paper for the final evaluation of DiD: *No safety layer/barrier of Defence-in-Depth introduces any risk addition and no safety layer/barrier reducing risk should be omitted.*

From what is said above, it is obvious from real accidents that DiD is either not properly defined or not properly applied, or both, since Fukushima happened after the recommendations related to DiD from INSAG 10 were adopted. So it seems that our "criticism" towards the currently defined DiD concept has reasons and agrees also with the following IAEA Convention on Nuclear Safety (IAEA [17]): "Implementation of safety improvements in relation to severe accident management has been an important issue since the 1970s. However the Contracting Parties have addressed the risks of severe accidents to different degrees and have different starting points for new assessments. The Fukushima Daiichi accident has provided impetus for the Contracting Parties to re-assess the safety measures in place at nuclear power plants in the context of natural events and to identify new measures that may need to be implemented."

3.1 Defence-in-Depth and physical safety barriers

3.1.1 Fuel matrix (core inventory)

Fuel matrix represents the first layer of DiD but it is not actually clear what is its role in the DiD. Indeed it does not include core inventory in the sense of its extent (amount) and quality (mix of radionuclides) which are the basis of the extent of source terms (radionuclide releases) and thus extent of possible releases depend on the core inventory extent. So, the only guaranteed way to reduce the maximum potential consequence part of risk stemming from severe accident is to reduce core inventory. With respect to the issue of core inventory and consequences, new trends are being developed based on the philosophy of Small Scale Reactors (Templinsky [18]).

3.1.2 Fuel cladding

Fuel cladding is supposed to be the second safety barrier of the currently understood DiD. Fuel cladding is mostly manufactured of zirconium alloy which has higher thermal conductivity in comparison to uranium dioxide. Nevertheless, the materials of cladding give rise to the risk of hydrogen production due to oxidation to which also hydrolysis of water is added, both exothermic reactions influencing the fuel and cladding (Gauntt *et al.* [35]). At the temperature over 1800°C H_2 production doubles and between 1800 and 1900°C it becomes

uncontrollable. Under these conditions core starts melting within 15 minutes Even though the cladding behaviour and risks related to H_2 production has been known since the beginning of nuclear industry, cladding was accepted as the second barrier of DiD.

3.1.3 Primary coolant boundary

Primary coolant boundary is considered to be the third safety barrier comprising the currently defined DiD concept. Primary coolant boundary is designed only for design basis accidents. Actually, in case of beyond design basis/severe accident its role as safety barrier is not guaranteed because of beyond design thermal and mechanical loads. Special features must be used in this case, as we could have seen actually in Fukushima case for direct core cooling through injection from e.g. firewater systems etc. On the other hand, coolant is the medium dedicated to remove the heat from the core, but in case of two loop nuclear power plants it is the secondary side, which is supposed to remove heat from the primary circuit and thus from the core. Secondary feedwater systems are counted as safety systems to cover various accidents and this is completely omitted in the structure of DiD.

3.1.4 Containment

Containment and reactor building are supposed to be the last engineering structures of the multiple-level DiD (INSAG-12 [1]). The components of a containment include: structures; isolating systems; penetrations and piping that constitute the containment boundary (Nuclear Safety Directorate UK [19]). Reference (Health and Safety Executive UK [20]) defines Principle P222, which indicates that "a containment and associated systems should be provided to limit radioactive releases under normal and fault conditions and to protect against hazards".

3.1.4.1 Containment vent systems Current trend foresees installation of vent systems in containment structures to reduce pressure loads to containment. In fact such modifications overturn the original function of the containment since these systems are purely containment protection-oriented while releasing radioactivity to the environment. This trend also proves that current containments, as they are currently designed, are not able to bear the pressure loads, which may occur during severe accidents as they were observed in Fukushima. It should be noted, that in Fukushima hard, not filtered vent systems were installed (Nuclear Safety Commission of Japan [21]) and in spite of nitrogen inertion inside of all the containments, hydrogen combustion/explosion occurred, since the hydrogen was vented directly into the reactor building where its concentration reached critical levels.

3.1.4.2 Containment leak tightness Containment should keep all accident resulting radioactivity inside. It is well known that a weak point of the VVER reactors is poor leak tightness of the confinement that results practically in very large leaks at all levels of any accident, even when no containment failure occurs. Thus, the usually presented 5% volume leak tightness per day of VVER

hermetic zones can vary up to the maximum allowed leak tightness, according to Technical specifications for VVERs 18vol. % per day. This aspect is omitted in DiD concept.

3.1.4.3 Safety barrier against underground leaks and leaks into waters As the Fukushima three year permanent leak into the Pacific shows, the barriers against radiological releases underground or into waters were not considered in the current designs. The corresponding safety layer is completely missing in the current safety analyses and DiD concept as well.

3.2 Defence-in-Depth and safety layers

3.2.1 Defence-in-Depth and conservative design

Conservative design refers strongly to fuel matrix/core and containment being the real physical structures designed to prevent and confine potential releases. The question with respect to "conservative" is, how much conservatism is sufficient to guarantee enough safety consistent with all IAEA safety objectives (INSAG-10 [12]) and principles (IAEA SF-1 [13]) The answer might be found in PSA results, since, according to IAEA (INSAG 12 [1]) PSA guides the design and operation. This means that PSA should be one of the safety layers confirming that the design is conservative enough to guarantee the safety, or rather risk minimization. In this respect, a proper analysis of PSA results is needed to answer the question. According to PSA L2 results that were performed by the authors of this paper for many plants, it can be summarized, that up to 90% of contribution to Large Early Release Frequency (LERF) can be expected from pure initiators with no other contributor regardless of any technical features. This is valid even in case of improvements and backfits of the plant that may show up to 50% of reduction in Core Damage Frequency (CDF), when only a marginal effect on LERF occurs. This implies that it is impossible to improve the current design towards reduction of risks from releases unless we reduce or eliminate some of the existing initiators. This follows actually from the fact, that none of the currently operating plants was designed to withstand severe accident conditions. Therefore, the layer of conservative design cannot be considered as safety layer at all.

3.2.2 Defence-in-Depth and human interactions

The DiD concept involves organizational and provisional measures and off-site emergency response all involving human interactions. This is covered for instance by one of the statements of European Nuclear Safety Regulators Group (ENSREG [22]): one of the most important lessons of abnormal events, ranging from minor incidents to serious accidents, is that they have often been the result of incorrect human actions. The evidence of the four severe accidents and the list of human errors prove this statement:

a) Bohunice A-1 Slovakia, 1977 (Kuruc and Matel [23], JAVYS [24]):
   The accident happened during refueling under operation and the main reason for the accident was officially reported as human error. The refueling crew, putting together an assembly, neglected to completely

clean the fuel assembly from the silica gel, which was used for dehumidifying the assembly parts for the duration of their transport. After putting the fuel assembly with the silica gel into the active zone, the silica gel restricted the flow of the cooling gas through this assembly.

b) TMI-2, USA, 1979 (US Nuclear Regulatory Commission [26]):
The officially declared reasons of the accident were a combination of human errors and a flawed PORV indicator light. The operators had not been trained to understand the ambiguous nature of the PORV indicator and to look for alternative confirmation that the main relief valve was closed.

c) Chernobyl, Ukraine/former USSR, 1986 (IAEA [25]):
This accident happened during an experiment, the major reason of the accident was reported as human error. During preparation and testing of the turbine generator under run-down conditions using the auxiliary load, personnel disconnected a series of technical protection systems and breached the most important operational safety provisions for conducting a technical exercise.

d) Fukushima, Japan, 2011 (National Diet of Japan [27]):
It was a profoundly manmade disaster – that could and should have been foreseen and prevented. It examines serious deficiencies in the response to the accident by TEPCO, regulators and the government. Its fundamental causes are to be found in the ingrained conventions of Japanese culture: our reflexive obedience; our reluctance to question authority. This conceit was reinforced by the collective mindset of Japanese bureaucracy, by which the first duty of any individual bureaucrat is to defend the interests of his organization. Carried to an extreme, this led bureaucrats to put organizational interests ahead of their paramount duty to protect public safety.

The currently used DiD concept overlooks the real evidence of accidents, where human errors – as in fact all PSA analyses prove – are the major basic events influencing accidents negatively both as initiators, or in the course of an accident involving not only plant personnel but also administrative personnel out of the plant as it happened in Fukushima. This should not be omitted together with the fact that human behavior is not reliable enough as safety layer of DiD being accompanied by too large uncertainties that introduce additional risks.

3.2.3 Defence-in-Depth and safety standards/criteria/goals

Basic acceptance criteria are usually defined as limits and conditions set by a regulatory body, and their purpose is to ensure the achievement of an adequate level of safety. These criteria are supplemented by other requirements to ensure DiD by, for example, preventing the consequential failure of a pressure boundary in an accident. (IAEA [28], 3.15) The most commonly used PSA safety criteria in particular countries are just frequencies in spite of the fact, that according to IAEA, the goal of PSA, as the driver of safe design, should be risk assessment. (INSAG-12 [1]) For L1 PSA the criterion is Core Damage Frequency – CDF, and for L2 PSA it is Large (Early) Release Frequency – L(E)RF. LERF is

considered to be sufficient for safety assessment of the plant even though it does not show "risk" as required by IAEA for PSAs.

Here several aspects are necessary to be analyzed:

- The gap in DiD with respect to safety/risk criteria
- Quality of risk criteria
- Common understanding of safety itself and risk criteria

As far as the first item – a layer of DiD provided by risk criteria is obviously missing from the currently defined DiD concept. As far as the second item (quality of risk criteria) it can be discussed on the background of Fukushima accident. The accident showed that even though all the Japanese authority's requirements were fulfilled, the accident still happened. This means, that in some respect the requirements and set criteria were not sufficient to prevent an accident of such an extent. On top of this, there is no common international understanding of safety as ascertained in many documents produced by major organizations and projects dealing with nuclear safety like ENSREG's stress tests, European Commission, SARNET, ASAMPSA2 etc. The authors of this paper developed a new Common Risk Target corresponding to internationally accepted IAEA safety objectives, safety principles, constant risk principle and IAEA graded INES scale taking into account Fukushima-like multiunit sites and fuel pool degradation. The details can be found in (Vitazkova and Cazzoli [29]).

The use of various criteria in different countries overlooks the need of uniform standards established already in 1996 after the Chernobyl accident. (INSAG-10 [12]): "The international consequences of the Chernobyl accident in 1986 have underlined the need for common safety principles for all countries and all types of nuclear power plants."

3.2.4 Defence-in-Depth and PSAs

3.2.4.1 Probabilistic and deterministic analyses PSA should guide design and operation, and thus PSA together with deterministic calculations are the only tools for the assessment of safety of a plant, which makes them the most important from among all the other concepts and strategies related to nuclear power plants safety. This factor is not considered in DiD layers at all.

3.2.4.2 PSA and risk assessment As stated above, PSA drives design and operation of nuclear power plants and it is considered to be a major tool for nuclear safety evaluation. PSA should be a comprehensive, structured approach identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. (IAEA SF-1 [13]) The total risk is the sum of the products of the consequences multiplied by their probabilities (INSAG-12 [1]).

Here the following aspects must be analyzed:

- The gap in DiD with respect to PSA
- Gap in PSA with respect to risk assessment
- Analysis of results in form of frequencies (focusing only on LERF)

The missing DiD "PSA layer" is obvious. Also, as the previously mentioned safety criteria prove, indeed not risk but frequencies are evaluated within PSAs. As far as analysis of results here the observation from section 3.2.1 with respect to major LERF contributors and possible backfits should be re-iterated.

3.2.5 Defence-in-Depth and uncertainties

To be aware what uncertainties mean, a comprehensive list of uncertainties covering several pages can be found in (IAEA [32]). Uncertainties at least for Level 2 are not included in the calculations in general (NUREG 1150 [33]). The currently proposed and applied uncertainty evaluation techniques are not yet integrated in the licensing process of many countries (IAEA [34]).

According to (IAEA [32]) the concept of "sufficient safety margin" stemming from deterministic analyses for design basis accidents is based on several levels, where experiments show much lower values (e.g. 1% claddings fail) in comparison to acceptance criteria (e.g. 10%) adopted by an authority which is still lower than supposed "threshold" safety limit (e.g. 20%). The following layout shows the safety margin approach including uncertainties and it shows that for a safe design the real/experimental value should be the lowest one followed by the upper uncertainty limit whereby both in turn should be below the acceptance criteria.

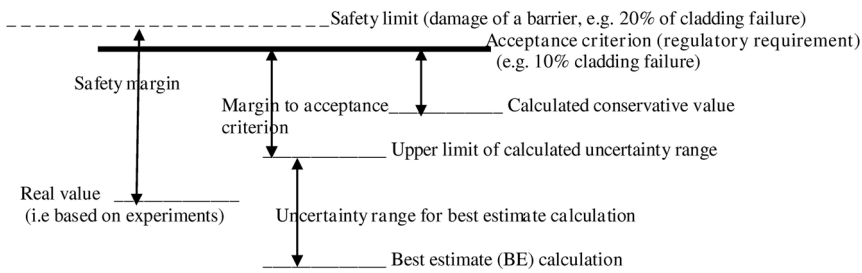

Figure 1: Safety margins with uncertainties in deterministic view.

Extrapolating this approach to PSA, the layout below is obtained considering real severe accidents. 4 core melts with large releases (1 x Chernobyl, 3 x Fukushima) in reported 14,500 reactor years (World Nuclear Association [36]) represent the "real" LERF equal to 2.8 E-4/Ry. Considering also the range of LERF objectives/limits in different countries (e.g. ASAMPSA2 [37]) the layout shows that the "real" value is much higher than both safety requirement and upper uncertainty limits, thus no "safety margins" are left in case of severe accidents. The reason is that currently operating plants were not designed to resist severe accident and this is discussed also in 3.2.1.

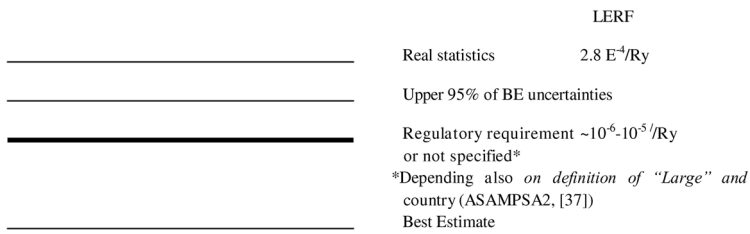

Figure 2: Safety margins with uncertainties in probabilistic view.

4 Conclusions

Based on the discussions in this paper it can be concluded that quite substantial changes should be made in the currently accepted DiD concept with respect to severe accidents. Note that most of the findings apply to new Generation IV designs too. The following shows a summary of the findings in the present paper:

DiD barriers:

1st barrier – Core inventory: reducing the maximum potential of risk either by reducing core size or the composition of the core – *add* this to DiD

2nd barrier – Fuel cladding: ignore this as safety barrier, since cladding represents significant additional risk source

3rd barrier – Secondary side/balance of plant add this to DiD as an important cooling factor.

4th barrier – Containment: *ignore* this as safety layer in case of venting
Need to define adequate and acceptably safe leak limits – *add* this to DiD
Underground leaks – no protection is considered in current DiD – *add* this to DiD
Leaks into waters/oceans – no protection is considered in current DiD – *add* this to DiD

DiD layers:

1st layer – Safety standards: missing in current DiD – add this to DiD
Risk criteria: (e.g. CRT (Vitazkova and Cazzoli [29])) complying with internationally accepted IAEA safety objectives and principles are missing in general and missing in current DiD too – *add* this to DiD
Commonly internationally accepted criteria are missing in general and in current DiD too – *add* this to DiD

2nd layer – PSA is missing in current DiD – add this to DiD
Risk assessment with full assessment of uncertainties (see also later) is missing in general and in current DiD too – *add* this to DiD

Analysis of current results with respect to LERF and basic events/initiators is missing in general and in current DiD too – *add* this to DiD

Uncertainties (consideration and interpretation of) are missing in general as part of PSA and in DiD too – *add* this to DiD

3rd layer – Conservative design – ignore this as safety layer for current plants because initiators and single errors occur in violation of IAEA safety principle 8 (IAEA [13]), and since no plant was designed for SAs, design cannot assure enough DiD out of principle

4th layer – Mitigation of consequences, organizational provisions, control – *ignore* these as safety layer because of two reasons:

- not corresponding to the source of radioactivity
- human errors are involved and they represent additional risk sources

References

[1] INSAG. *Basic Safety Principles for Nuclear Power Plants*, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[2] IAEA, http://www-ns.iaea.org/standards/concepts-terms.asp

[3] IAEA, http://www.iaea.org/ns/tutorials/regcontrol/assess/assess3213.htm

[4] Naukova Dumka. *Chernobylskaia Katastrofa Bariachtara*, Kiev, 1995.

[5] Aleksakhin, R.M, *et al*. *Radiacijonnyje avarii,* Pod redaktsiyey akademika RAMN Iljina, L.A and Gubanova, V.A, Moskva Izdat, 2001.

[6] Ministry of Ukraine of Emergencies. *Twenty-five Years after Chornobyl Accident: Safety for the Future, National Report of Ukraine*, Kyiv, 2011, UDK 621.311.25:621.039.586/(477.41-21), BBK 31.47 (4Ukr-4kij)-08 D22.

[7] http://ru.wikipedia.org/wiki/%D0%9B%D1%83%D1%87%D0%B5%D0%B2%D0%B0%D1%8F_%D0%B1%D0%BE%D0%BB%D0%B5%D0%B7%D0%BD%D1%8C, Lučevaja boleznj.

[8] IAEA, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1239_web.pdf

[9] Ministry of Ukraine of Emergencies and Affairs of Population Protection from the Consequences of Chornobyl Catastrophe. *ATLAS Ukraine Radioactive contamination*. Intelligence Systems GEO, Ltd., Kyiv, 2008.

[10] Shestopalov, V.M, Naboka, M.V. *Medical Consequences of the Accident at CHNPP*. Chornobilskiy naukovyj visnik, Bjuletenj ekologichnogo stanu zony vidchuzhenija, 25 rokovini Chornobilskoj katastrofi, No. 1 (37) 2011.

[11] IAEA. *Chernobyl's Legacy: Health, Environmental and Socio-Economic Impacts and Recommendations to the Governments of Belarus, the Russian Federation and Ukraine*. The Chernobyl Forum 2003–2005.

[12] International Nuclear Safety Advisory Group. *Defence in Depth in Nuclear Safety*, INSAG-10, IAEA, Vienna 1996.

[13] IAEA. *Fundamental Safety Principles, Safety Fundamentals No. SF-1*, ISBN 92-0-110706-4, ISSN 1020-525X, Vienna, 2006.
[14] SNETP. *Identification of Research Areas in Response to the Fukushima Accident*. Report of the SNETP Fukushima Task Group, Chairman Jozef Misak, January 2013.
[15] IAEA. *Safety of Nuclear Power Plants: Operation*, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna 2000.
[16] European Commission. *Communication from the Commission to the Council and the European Parliament on the interim report on the comprehensive risk and safety assessments ("stress tests") of nuclear power plants in the European Union*, COM(20110 784 final, SEC(2011) 1395 final, Brussels, 24.11.2011.
[17] Convention on Nuclear Safety, http://www-ns.iaea.org/conventions/nuclear-safety.asp
[18] Templinsky, E. Pillsbury. *Latest Trends and Developments for Small Scale Nuclear Reactors*, Kuala Lumpur, Malaysia, January 15–16, 2013.
[19] Nuclear Safety Directorate UK. *Technical Assessment Guide – Containment for reactor plant*, T/AST/20, Issue No. 002, April 2008.
[20] Health and Safety Executive. *Safety Assessment Principles for Nuclear Plants*, ISBN 0 11 882043 5, 1992.
[21] The Nuclear Safety Commission of Japan. *NSCRG: L-AM-II.0.1 Accident Management for Severe Accidents at Light Water Power Reactor Installations*, May 1992.
[22] ENSREG, http://www.ensreg.eu/nuclear-safety
[23] Kuruc, J., Matel, L. *Thirtieth Anniversary of Reactor Accident in A-1 Nuclear Power Plant Jaslovske Bohunice*, Minulosť a súčasné trendy jadrovej chémie, Omega Info, ISBN 978 80 969290 9 2, 2007.
[24] JAVYS (Nuclear Decomissioning Society in Slovakia), http://www.javys.sk/en/nuclear-facilities/a1-nuclear-power-plant/history
[25] INSAG-1. *Summary Report on the Post-Accident Review on the Chernobyl Accident*. Safety Series No. 75-INSAG-1.IAEA, Vienna, 1986.
[26] US Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html
[27] The National Diet of Japan. *The official report of the Fukushima Nuclear Accident Independent Investigation Commission*, Executive Summary, 2012.
[28] IAEA. *Deterministic Safety Analysis for Nuclear Power Plants*, Specific Safety Guide No. SSG-2, IAEA, Vienna 2009.
[29] Vitazkova, J., Cazzoli, E. *Common Risk Target for severe accidents of nuclear power plants based on IAEA INES scale.* Nuclear Engineering and Design, Vol. 262, Pages 106–125; ISSN 0029-5493, September 2013.
[30] IAEA Safety Standards for protecting people and environment. *Governmental, Legal and Regulatory Framework for Safety. General Safety Requirements Part 1*. No. GSR Part 1, Vienna, 2010.

[31] National Aeronautics and Space Administration. *General Safety Program Requirements*, NPR 8715.3C, Office of Safety and Mission Assurance, March 12, 2008.
[32] IAEA. *Safety Report Series No. 52, Best estimate Safety Analysis for Nuclear Power Plants: Uncertainty evaluation; Vienna 2008.*
[33] US Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants*, *(NUREG 1150),* December 1990, US NRC, Division of Systems Research, Office of Nuclear Regulatory Research, Washington DC.
[34] IAEA. TECDOC-1332, *Safety margins of operating reactors Analysis of uncertainties and implications for decision making*, IAEA January 2003.
[35] Gauntt, R.O. *et al*. *MELCOR Computer Code Manuals: Version 1.8.5*, NUREG/CR-6119, 2000.
[36] World Nuclear Association, www.world-nuclear.org
[37] Seventh Framework Programme Advanced Safety Assessment Methodologies, Nuclear Fission, Safety of Existing Nuclear Installations, Level 2 PSA (ASAMPSA2). *Best Practices Guidelines for L2 PSA development and applications*, Contract 211594; Technical Report ASAMPSA2 WP2-3-4/D.33/2013/35, IRSN PSN-RES/SAG/2013-177, Vol. 1–2, 2013.