Modern Environmental Science and Engineering (ISSN 2333-2581)
October 2017, Volume 3, No. 10, pp. 724-732
Doi: 10.15341/mese(2333-2581)/10.03.2017/007
Academic Star Publishing Company, 2017
www.academicstar.us

Updating of a Screening Method for Assessment of Comprehensiveness of Defence in Depth and Areas for Its Applications

Jozef Misak

UJV Rez, a.s. (Nuclear Research Institute), Czech Republic

Abstract: The paper describes the updated IAEA screening method for assessment of comprehensiveness of defence in depth for both existing as well as new nuclear power plants. In its first part the paper briefly summarizes the original IAEA method developed more than 10 years ago, described in the IAEA Safety Report No. 46 — Assessment of defence in depth for nuclear power plants. Further on, the need for updating the methods is justified making reference to relevant new IAEA Safety Standards and other guidance documents used for updating the method with consideration of new safety requirements and main directions in safety enhancement. Key modifications in the original IAEA method of objective trees are summarized. An example of the updated objective tree is provided and compared with the original tree. In the last part of the paper the potential areas for the use of the method areindicated.

Key words: nuclear power plants, defence in depth, screeing method, objective trees

1. Introduction

As reconfirmed by different forums, defence in depth based on multiple barriers and variety of means (provisions) to protect the barriers is and should remain an essential strategy to ensure nuclear safety for both existing and new nuclear power plants (NPPs).

Since many years, defence in depth represents a focal point for IAEA safety related activities. The need for a practical tool aimed at facilitating assessment of comprehensiveness of defence in depth has been recognized by the IAEA at the end of 90-ties with the objective to contribute to more specific understanding of this very general term: all NPPs have physical barriers and means to protect the barriers, while their level of defence in depth can be very different.

Among many IAEA documents related to defence in depth there are two documents with special importance for the present report. One of them is INSAG-12 (update of INSAG-3) — Basic Safety Principles for NPPs, published in 1999 [1], introducing the concept of basic safety principles as necessary conditions for ensuring plant safety, and Safety Report No. 46 — Assessment of defence in depth for NPPs, published in 2005 [2], which describes a screening method for assessing comprehensiveness of the defence in depth capabilities of a NPP (mainly of an existing plant), including all necessary measures taken to ensure safety. Since development of Safety Report No. 46 significant enhancement in international safety requirements including also enhancement of defence in depth took place, in particular after the Fukushima accident. For further use of the Safety Report No. 46 it is therefore necessary to update the report taking into account all new safety developments and also to improve user friendliness of the method based on experience from its previous applications.

In 2016, the Czech electric utility CEZ a.s. decided to update the method of objective tress with due

Corresponding author: Jozef Misak, Dr.; research areas/interests: nuclear engineering/nuclear safety. E-mail: Jozef.Misak@ujv.cz.

consideration of all new safety requirements with the aim to use the method in next periodic safety reviews of NPPs in the Czech Republic. The updated methodology should provide a tool for periodic safety assessment of operating NPPs in the scope defined in the IAEA Specific Safety Guide SSG-25 — Periodic Safety Review for Nuclear Power Plants [3].

The paper describes the updated screening method developed in response to the CEZ decision. In its first part the paper briefly summarizes the original IAEA method as described in Safety Report No. 46. Further on, the need for updating the method is justified making reference to the relevant new IAEA Safety Standards and other international guidance documents. Key modifications in the original IAEA method of objective trees are summarized. An example of the updated objective tree is provided. It is obvious that the use of the method can be much broader than just to be a tool for performing the periodic safety review. In the last part of the paper such potential areas for the use of the method are presented.

The updated method is intended to be predominantly used by the operating organization, and therefore the provisions for ensuring safety are focused on those which can be managed by the operating organization.

It is assumed that the IAEA can provide a forum for further improvement of the method and its broader distribution and utilization by the Member States.

2. Brief Description of the Method of Objective Trees

IAEA Safety Report No. 46 describes the reference approach for checking the completeness and quality of implementation of the concept of defence in depth in a systematic way. The bases for the approach were as follows:

- Safety should be ensured by implementing safety provisions at all 5 levels of defence in depth at any time;
- Each of the levels should be individually robust;
- Each level has its relevant safety objectives ensured by corresponding integrity of the physical barriers;
- For maintaining integrity of the barriers, the fundamental safety functions (FSFs) and more detailed (derived) safety functions (SFs) should be performed;
- SFs can be challenged by a number of mechanisms affecting their performance;
- To prevent mechanisms affecting the SFs, safety provisions of different kinds should be implemented;
- Provisions implemented at different levels of defence should be reasonably independent.

The concept of defence in depth has been often oversimplified and misinterpreted just as a set of physical barriers, whose integrity is ensured by safety provisions as the plant systems (hardware provisions) implemented at various levels of defence. However, comprehensive measures to ensure effectiveness of the barriers against releases of radioactive substances should include much broader variety of safety provisions: organizational, behavioural and design measures, namely inherent safety characteristics; safety margins; active and passive systems; operating procedures and operator actions; human factors and other organizational measures; safety culture aspects. It is important to underline that although plant technological systems are very important, they are not the only components of defence in depth.

The screening approach described in the IAEA Safety Report No. 46 uses so called objective trees (Fig. 1) for screening the availability safety provisions at five levels of defence. The top down approach has been used for the development of objective trees, i.e., from stating the objectives and relevant SFs for each level of defence, through the challenges to performance of these SFs composed of various mechanisms affecting the performance, up to the provisions which may be implemented to prevent challenges to SFs to take place. The provisions are aimed at preventing the mechanisms

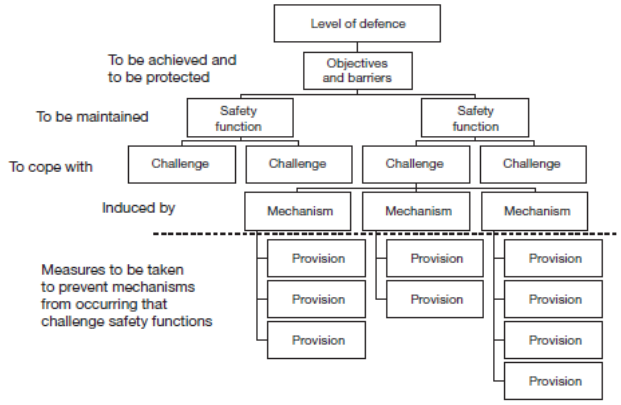

Fig. 1 Illustrative structure of the objective tree at each level of defence.

and challenges to SFs to take place so that to ensure integrity of physical barriers and achieving safety objectives at each level of defence.

Graphical depiction of links between safety objectives and safety provisions in the form of an objective tree helps to identify weaknesses in defence in depth and supports the questioning attitude essential for nuclear safety. Screening by means of objective trees should be understood not only as a comprehensive tool for assessment, but also as a way of thinking on nuclear safety in very broad circumstances.

Nevertheless it should be mentioned that the approach described in Safety Report No. 46 does not include any quantification of the extent of defence in depth nor prioritization of the provisions of defence. The approach is intended only for screening, i.e., for identification of both the strengths and weaknesses and for identification which additional provisions could be considered. There are no criteria on what is considered a sufficient level of implementation of individual provisions. The level of detail and completeness of evaluation are at the discretion of every user of the approach.

Use of the method for checking comprehensiveness of defence in depth is done in a reverse way compared to development of the method, it means by bottom up of screening of individual provisions, including the following steps:

- Comparison of provisions specified in the objective trees with capabilities of the plant;
- Judgment of the level of implementation of each provision in siting, design, construction, commissioning and operation;
- Consideration of optional provisions and judgment whether an absence of a provision leads to the weakness in defence in depth;
- Judgment whether a mechanism can be considered as prevented to occur;
- Judgment whether a challenge can be considered as prevented to affect fulfillment of a safety function.

In summary, the objective trees in the IAEA Safety Report No. 46 included 95 different challenges (some of them applicable for several levels), 254 different mechanisms and 941 different provisions. It will be shown further in the paper that updating the Safety Report No. 46 will lead to significantly increased number of items in the objective trees.

3. The Need for Updating the Method for Assessment of Comprehensiveness of Defence in Depth

The Fukushima accident demonstrated importance of comprehensive implementation of defence in depth and reactivated interest in various methods for its assessment. There was the IAEA International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety held in Vienna, 21-24 October 2013 [4]. Among conclusions of the conference there was a confirmation of importance and value of defence in depth for both existing and new plants. Further development of the tools based on the methodology described in the Safety Report No. 46 was recommended as a means for ensuring that defence in depth safety provisions are comprehensive enough. In the conclusions of the conference a number of recommendations were presented with the objective of further strengthening the defence in depth. Among the

recommendations there was also the need to take into account the most recent IAEA Safety Standards and maintenance of compliance with these Standards by periodic safety reviews over the entire life of the plants. The need for further development of guidance documents and tools for assessment of required new features of defence in depth was also included in the recommendations.

Following the conference, there were several meetings organized by the IAEA partially addressing the defence in depth, but no specific actions on updating of Safety Report 46 were taken up to now.

In 2016, the Czech utility CEZ a.s. decided to use the method of objective tress described in IAEA Safety Report No. 46 for assessment of the level of defence in depth in next periodic safety reviews of Czech NPPs. It was clear that the original objective trees developed more than 10 years ago needs updating in order to reflect all relevant new safety requirements as well as to improve user friendliness of the method. The updating has had also to reflect on-going updating of the Czech nuclear legislation.

It was clear from the beginning that the update will significantly influence the original scope and level of detail of the screening method described in IAEA Safety Report No. 46. For demonstration of the needed scope of updating, the key enhancements to be incorporated based on IAEA Safety Requirements are summarized below.

Main areas of strengthening in the IAEA Safety Requirements for siting include the following items [5]:

- The need to evaluate frequency and severity of external natural and human induced events, with consideration of potential combination of events;
- Establishing the design basis hazard level considering frequency and severity of events with associated uncertainties, considering long term historical data;
- Assessment of the feasibility of implementation of emergency plans, considering potential mutual effects among multiple nuclear and other facilities at one site;
- Periodic review of site specific hazards (every 10 years or shorter in case of significant changes in hazards) with evaluation of implications.

Main areas of strengthening in the updated Safety Requirements for design [6] are as follows:

- Consideration in the plant design of all plant states up to design extension conditions including severe accidents in the plant design envelope;
- Limitation of radiological consequences of accident conditions: no off-site measures needed for any design basis accidents, of-site measures limited in area and time for severe accidents, which are not practically eliminated;
- Strengthening the plant design basis by consideration of external hazards with implementation of sufficient margins;
- Practical elimination of unacceptable radiological consequences (elimination of early or large radioactive releases) to the public and the environment (elimination or minimization of site contamination);
- Reinforcement of the independence of defence in depth provisions, in particular between levels 3 and 4 — implementation of dedicated safety provisions for design extension conditions;
- Stressing the need for margins to avoid cliff edge effects;
- For items that ultimately prevent large or early releases more margins are required, also for external hazards more severe than those selected for the design basis;
- In a multiunit site, each plant unit to have its own safety systems and safety features for design extension conditions, but considering

interconnections between the units for enhancement of safety;
- Reinforced capabilities for heat transfer to the UHS; alternative heat sink or different heat transport route is required for conditions generated by beyond design basis external events;
- Strengthening design of the control room with margins against natural hazards exceeding the design basis;
- Implementation of features to enable the use (e.g., hook-up) of non-permanent equipment;
- Reinforced capabilities for power supply in design extension conditions; independent and separated alternate power sources for station black-out accidents, with continuity of power for monitoring;
- Emergency response facilities capable to withstand conditions generated by accidents and hazards;
- Additional measures for spent fuel pool (SFP) monitoring (temperature, water level, activity, water chemistry), cooling and maintaining inventory including use of non-permanent equipment (in order to practically eliminate severe accidents).

Main areas of strengthening in the updated Safety Requirements for operation [7] are as follows:
- Periodic safety review to consider national and international experience, national and international standards and to cover site related aspects;
- Implementing corrective actions and reasonably practicable modifications to reduce likelihood and potential consequences of accidents;
- Strengthening means of communication, availability of information in emergency response facilities and locations with regular testing, validation and training on emergency preparedness;
- Strengthening accident management, degraded regional infrastructure and adverse working conditions, ensuring safe location and maintenance of non-permanent equipment;
- Periodical review and revisions of accident management programme;
- For multiunit sites considering concurrent accidents affecting all units with verification of availability of experienced personnel, equipment, supplies and external support;
- Considering contingency measures such as an alternative supply of cooling water and an alternative supply of electrical power to mitigate the consequences of accidents;
- Ensuring safe and accessible storage of temporary equipment;
- Appropriate competences, systems and technical support, with adequate validation, testing and exercises of accident management, including long-term actions;
- Feedback from operating experience to include emergency responses and lessons learned from other industries;
- Establishing maintenance programmes, training and exercises for no-permanent equipment.

In addition to the IAEA Safety Requirements, other documents taken into account in updating the screening method of the objective trees include:
- IAEA Report on Human and Organization Factors in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [8]
- IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [9]
- Post-Fukushima updating of WENRA reference levels for existing reactors [10]
- Recommendations from the post-Fukushima stress tests, in particular from the EU stress tests [11, 12],

- OECD/NEA lessons learned from Fukushima accident published in 2016 in document [13].

All these reference documents in combination with accumulated experience from the previous use of the method were used in systematic updating of all objective trees included in Safety Report No. 46, so that all new safety requirements are now adequately covered.

4. Comparison of Objective Trees in Original IAEA Methodology and Newly Developed Objective Trees

It is clear that the most significant changes in the objective trees resulted from the new safety requirements as well as from the accumulated experience from previous applications of the method. However, it was also necessary to improve user friendliness of the original method. Development of objective trees in Safety Report No. 46 was significantly limited by available hardware and software computational means at the time of the development. The software system had limited flexibility, size of the boxes in the objective trees did not allow to insert sufficiently self-understandable text of provisions, etc. The whole set of objective trees remained just in the paper form, not allowing any further development and improvements. Rigid structure of the objective trees with no flexibility was the main obstacle is broader use of the method.

Old objective trees were developed in Microsoft PowerPoint 97-2003 software. New objective trees are developed in two formats. One of the formats are standard excel tables, easy to be updated and also providing certain visualization of the objective trees. The second format has a typical shape of a tree produced by the Microsoft Office Visio 2007 or Microsoft Excel 2010 software tool. Challenges, mechanisms and provisions are more specifically and therefore more understandably formulated. A specific set of provisions is associated with each individual mechanism differently from the past when the same more general provisions were associated with several mechanisms at the same time. Currently available software also allows adding to individual items in the objective trees various attributes of the items as appropriate, such as numbering of provisions or their linking to more specific safety requirements. The available software offers a reasonably simple transfer of an objective tree developed in an excel table into a Microsoft Visio or Excel figure and vice versa.

The overall effect of updating of objective trees can be illustrated by some numbers showing that in comparison with Safety Report No. 46 the number of challenges included in the objective trees increased from 95 to 128, number of mechanisms from 254 to 347 and number of indicated provisions to prevent mechanisms challenging the safety functions was nearly doubled, with increase from 941 to 1797.

All objective trees from the original Safety Report No. 46 were transferred into a new format in excel sheets, thus allowing improving and updating the objective trees taking into account information from various reference sources in the present report. Practically all objective trees were expanded to provide adequate level of details and to reflect new requirements. Some new objective trees were added to reflect completely new requirements, for example the tree for assessment of practical elimination of early or large radioactive releases. The objective trees are at present being verified by CEZ experts in various fields of nuclear safety. It would be very appropriate to involve the IAEA experts in the process thus to improve overall quality and applicability of the method.

The changes discussed above are illustrated in the figures below. Fig. 2 shows one of the “old” objective trees corresponding to the safety principle “Station blackout”, while Fig. 3 shows the equivalent updated excel table and Fig. 4 the new objective tree corresponding to the same safety principle.

These examples demonstrate significant technical enhancements as well as improvements in user

friendliness of the method thus providing better conditions for broader use of the method. Similar modifications, although not necessarily so significant, were implemented in all objective trees of IAEA Safety Report No. 46.

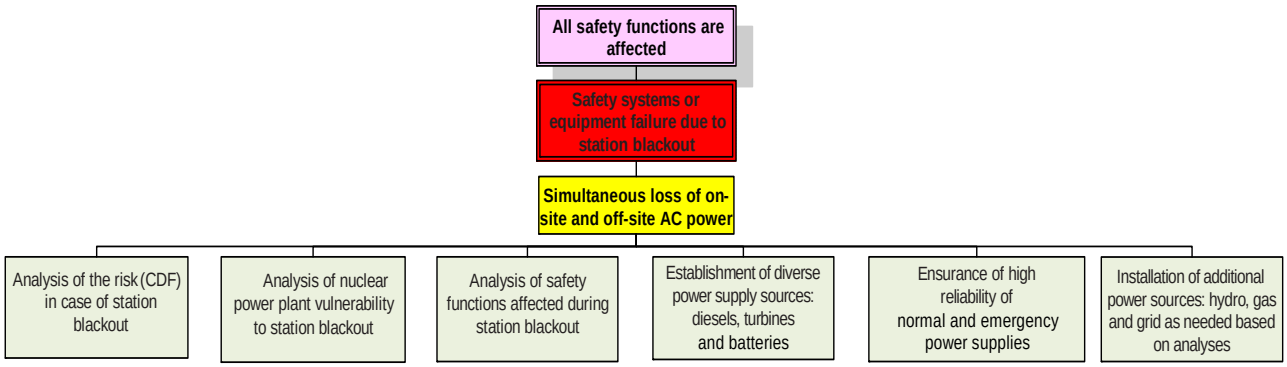

Fig. 2 Objective tree corresponding to the safety principle "Station blackout" in IAEA Safety Report No. 46.

Safety principle -	Challenge - text	Mechanism - text	Provision 1	Provision 2	Provision 3	Provision 4	Provision 5	Provision 6	Provision 7	Provision 8	Provision 9
Station blackout	Safety systems or equipment unavailable due to station blackout	Plant vulnerability to SBO large or unknown	Overview of vulnerabilities under different plant conditions	Assessment of time windows for connection of alternative sources	Assessment of the risk and implications of the RCP seal damage	Identification of means for enhancing capability to withstand SBO					
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO coping capability inadequate	Capability of the turbine island to handle large load rejection	Multiple grid connections at different voltage levels including secure connections	Nearby hydro or a gas power plant, having a black start capability	Alternate AC power source designed for anticipated external events	Nearby hydro or a gas power plant, having a black start capability	Dedicated small AC power sources for specific functions such as battery charging	Mobile diesel / gas turbine generators (medium or low voltage)	Trailer mounted fuel tanks, hoses, fuel transfer pumps, and cable spools	High capacity station batteries (e.g. 12-24 hours) or additional spare battery systems
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to unavailability of information about	Assessment of vulnerabilities of key plant instrumentation under SBO conditions	Procedures for extrapolation of data from remaining instrumentation	Use of dedicated sources of power and coolant with their own instrumentation	Assessment of accessibility of field measurement points	Use of portable self-powered measuring equipment				
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions unavailable due to damage of equipment or infrastructure	Storage of equipment in spaces resistant against earthquakes and flooding	Storage of equipment in light structures minimizing damage of stored equipment	Storage of equipment in different places minimizing risk of damage by same event	Installing water-proof doors sealing the electrical compartments	Sealing external cable raceways to prevent water intrusion	Modifying the plant for connecting alternative sources of power and coolant	Debris removal machines stored in protected areas	Dewatering pumps to remove water frpm areas requiring access	
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to lack of external support	Provisions for coordination, accepting, deploying off-site resources	Staging areas to receive equipment from off-site resources	Coordination agreements with potential off-site supports	Establishment of regional centers with technical and human resources	Database with external resources capable of supporting plant needs				
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to poor staff performance	Development of accident management strategies for SBO conditions	Development of procedures for actions needed for extended SBO	Improved procedures for restoring the offsite power or connection nearby units	Load shedding procedures to extend battery discharge time	Procedures to connect and power specific buses, operate switches and breakers	Validation of procedures for accomplishment within expected times under harsh conditions	Training of personnel for manual actions needed in case of SBO	Drills that encompass full sequences, including connections of non-permamanet equipment	Portable battery or diesel powered lights
Station blackout	Safety systems or equipment unavailable due to station blackout	SBO provisions ineffective due to short mission time	Analysis of limitation of mission time by availability of consumables	Increased on-site availability of consumables (oil, lubrication)	Provisions to replenish consumables for indefinite mission time						

Fig. 3 Excel table corresponding to the objective tree for the safety principle "station blackout".

5. Potential Applications of the Method

There were examples of application of the objective trees approach in the past and renewed interest in the approach is observed after the Fukushima Daiichi accident. The applications until now demonstrated that the screening method is based on a sound concept and can be effectively used by NPPs, that it helps identifying missing or weak provisions, that understanding of importance of provisions and interactions among provisions/mechanisms by using the method is improved because of complexity and visualization in the form of objective trees, and that self-assessment mode of the review contributes to the safety culture-questioning attitude of the reviewers. The updating of the method by incorporating all new safety requirements and improvements of user friendliness of the method provides a good basis for broader use of the method.

Following applications of the methods may be considered:

- Bottom-up qualitative assessment of availability of identified provisions in any specific NPP, combined with an expert judgments of sufficiency of provisions for preventing challenges to safety functions to take place;
- Use of selected lists of provisions as reminders for verification of availability of necessary measures in specific safety reviews, including IAEA safety review missions;
- Verification of comprehensiveness of safety assessment criteria in periodic safety reviews by comparing the criteria with the list of provisions identified in the objective trees;

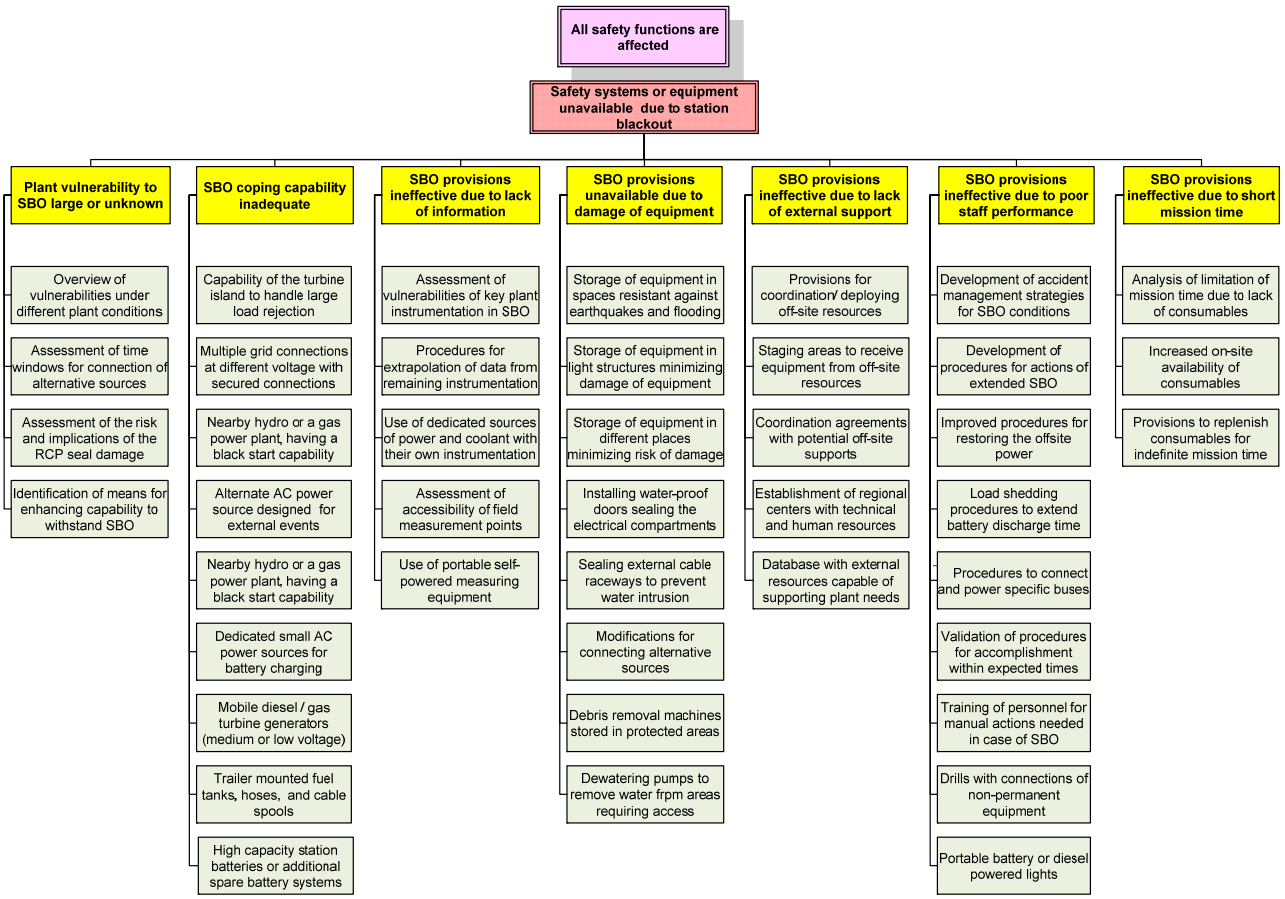

Fig. 4 Updated objective tree corresponding to the safety principle "Station blackout".

- Assessment of severity of deficiencies in safety level identified in periodic safety review by indicating the challenges to performance of safety functions, levels of defence in depth affected and available provisions possibly compensating the deficiencies;
- Use of identified gaps in comprehensiveness of defence in depth provisions for identification of measures for safety upgrading of the NPPs;
- Demonstration of progress in safety upgrading of a given NPP by increasing the number and level of implementation of different safety provisions;
- Demonstration of a comprehensive consideration of defence in depth in the plant Safety Analysis Reports;
- Use the objective trees for training of NPP staff in comprehensive consideration of defence in depth in their day by day operations.

6. Conclusions

The IAEA Safety Report No. 46 provided a feasible framework for assessment of comprehensiveness of implementation of defence in depth provisions, but due to relatively long time since its publication it needed updating and improvements of its user friendliness. The work described in the paper responded to the needs for overall improvements of the whole methodology for screening comprehensiveness of the defence in depth at all levels of defence.

Updating of the challenges, mechanism and provisions in the objective trees took into account strengthening of international and national safety requirements and lessons learned, in particular those reflected in the IAEA Safety Standards, WENRA reference levels and safety objectives, OECD/NEA recommendations for strengthening of defence in depth,

and any other post-Fukushima lessons learned, including results of the European and other stress tests.

In the updated method, the original basis of the approach by means of systematic assessment of provisions available to prevent mechanisms and challenges affecting safety functions potentially leading to the damage of the barriers against releases of radioactivity was maintained. The way of illustrating the links between safety objectives, barriers, safety functions, challenges, mechanisms and safety provisions by graphically presented objective trees remained unchanged, providing additional possibility of presenting objective trees in the format of excel sheets easy to be updated.

The updating also included adjustment of the balance between individual objective trees, as well as checking and improvements of the formulation of the items in the objective trees to ensure their validity, correctness and clarity of the formulations.

The user friendliness of the method was improved by developing a computerized version of objective trees, with sufficient flexibility for further corrections and modifications, with a possibility to associate various attributes to individual items of the objective trees, with a possibility of easy updating the objective trees.

Czech electric utility CEZ a.s., offers the method for further international adaptation and broader use for assessment. IAEA is invited to provide the framework for broader international use of the method.

Acknowledgements

The paper has been prepared in close cooperation with the staff of engineering department of the Czech electric utility CEZ a.s.

References

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

[2] IAEA, *Assessment of Defence in Depth for Nuclear Power Plants*, Safety Report Series No. 46, Vienna, 2005.

[3] IAEA, *Periodic Safety Review for Nuclear Power Plants, Specific Safety Guide*, SSG-25, Vienna, 2013.

[4] IAEA, *International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety*, Vienna, 21-24 October, 2013.

[5] IAEA, *Site Evaluation for Nuclear Installations, Specific Safety Requirements*, NS-R-3, Rev. 1, Vienna, 2016.

[6] IAEA, *Safety of Nuclear Power Plants: Design, Specific Safety Requirements*, SSR-2/1 Rev. 1, Vienna, 2016.

[7] IAEA, *Safety of Nuclear Power Plants: Commissioning and Operation, Specific Safety Requirements*, SSR-2/2, Rev. 1, Vienna, 2016.

[8] IAEA, *Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting*, Vienna, Austria, 21-24 May, 2013.

[9] IAEA, *Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant*, 2013

[10] WENRA, Safety Reference Levels for Existing Reactors — Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, September 2014.

[11] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Overview and Conclusions, Presented to ENSREG by the Peer Review Board, April 2012.

[12] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, Presented to ENSREG by the Peer Review Board, July 2012.

[13] *Implementation of Defence in Depth at Nuclear Power Plants — Lessons Learnt from the Fukushima Daiichi Accident*, OECD/ NEA No. 7248, 2016.