Application of FIRE PSA in case of modifications for post-operational shutdown states

Türschmann, Michael, Babst, Siegfried*, Röwekamp, Marina***

*Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH,
Kurfürstendamm 200, 10719 Berlin, Germany
** Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH,
Schwertnergasse, 50667 Köln, Germany

Abstract:
This contribution presents results of recent research and development activities in the field of Hazards PSA (HPSA). The reactor accidents at Fukushima Dai-ichi in March 2011 gave reason and indications for checking the risk assessment approach for internal and external hazards as currently described in the German PSA Guideline and its supplementary technical documents. A standardized approach for performing a comprehensive HPSA has been developed emphasizing the complete consideration of all potential failure dependencies induced by hazards. The systematic extension of the given plant model of Level 1 PSA is the real crux of the new HPSA approach. The extension is carried out for each hazard *H* using the corresponding Hazard Equipment List (*H-EL*) and the corresponding Hazard Dependency List (*H-DL*). Parts of the approach have already been tested.
In the paper a successful application for the plant internal hazard fire is presented. A German licensee plans a system modification of the spent fuel pool cooling, therefore a Level 1 PSA has been carried out to compare the fuel damage frequencies for the existing and the modified version. It is described how the systematic (and partly automatic) extension of the fault trees is performed using the Fire Equipment List (*F-EL*). The *F-EL* contains a compartment assignment for all relevant components and cables. The probability of a room failure by fire must be determined for any mapped room. This is the conditional probability that the components and cables within the room are destroyed by the fire.

1 INTRODUCTION

The German PSA Guideline [1] and its supplementary technical documents on PSA methods [2] and data [3] require probabilistic safety analyses (PSA) to be carried out in the frame of safety reviews for nuclear power plants (NPP). Since 2005, this also covers probabilistic analyses for internal and external hazards. For performing safety analyses, for some of these internal and external hazards (fire, internal flooding, aircraft crash, explosion pressure wave, external flooding, earthquake) specifications and methodological approaches are provided in the document on PSA methods [2] supplementing the PSA Guideline. The risk contribution of other external hazards such as toxic gas clouds, external fires, ship collisions with intake structures, extreme weather conditions and biological phenomena have to be only roughly estimated.
The Fukushima Dai-ichi reactor accidents in March 2011 gave reason and indications for checking again models and results with respect to risk assessment of external hazards. Meanwhile, it is recommended that the safety assessment of a nuclear power plant (NPP) does also cover a comprehensive Level 1 PSA for all internal as well as site specifically identified and evaluated external hazards (HPSA).
A standardized approach for performing a comprehensive HPSA has been developed for all kinds of internal and external hazards. The approach emphasizes the complete consideration of all potential dependencies (impact dependencies of different hazards, dependencies of safety functions needed to control the consequences of hazard induced initiating events and dependencies of hazard induced failures of structures, systems and components) in the plant quantification model.

The systematic - and for the most part automatic - extension of the given plant model of Level 1 PSA is the real crux of the new approach. The extension is carried out using hazard equipment lists (*H-EL*) and hazard dependency lists (*H-DL*). The lists are generated supported by a database.
Meanwhile, some parts of the approach have already been tested, e.g. the database-supported generation of *H-EL* (in particular, the generation of a seismic equipment list, *S-EL* [4]) and the automatic extension of fault tree models using the information of a fire equipment list, *F-EL*.
Following, the general approach of a systematical compilation of *H-EL* and *H-DL* and the use of these lists to extend a given Level 1 plant model is outlined. The application of this concept is shown for a probabilistic fire risk analysis.

2 SYSTEMATIC EXTENSION OF THE LEVEL 1 PSA PLANT MODEL

The general approach for a systematical compilation of *H-EL* and *H-DL* is explained at length in [6] (see also Figure 1). In the following, a short overview is given focussing on the systematic extension of Level 1 PSA model. A practical application is given in chapter 3.

For a given NPP site, the contribution of internal and external hazards to the overall risk is to be assessed by means of Hazards PSA (HPSA). For that purpose, it is assumed that a PSA for plant internal initiating events (IE) does exist. This means in particular that a plant risk model - consisting of event and fault trees - has been derived in order to calculate the risk (e.g. core damage frequency in case of Level 1 PSA) and is available for further use. The basic events of this Level 1 plant risk model are mainly failures, malfunctions or unavailabilities of technical components and human errors. The model extensions also refer to failures or unavailabilities of buildings and their structural elements (e.g. rooms, walls, distribution systems such as pipes or cables). The systematic performance of a HPSA comprises modeling on three different levels (see Figure 1).

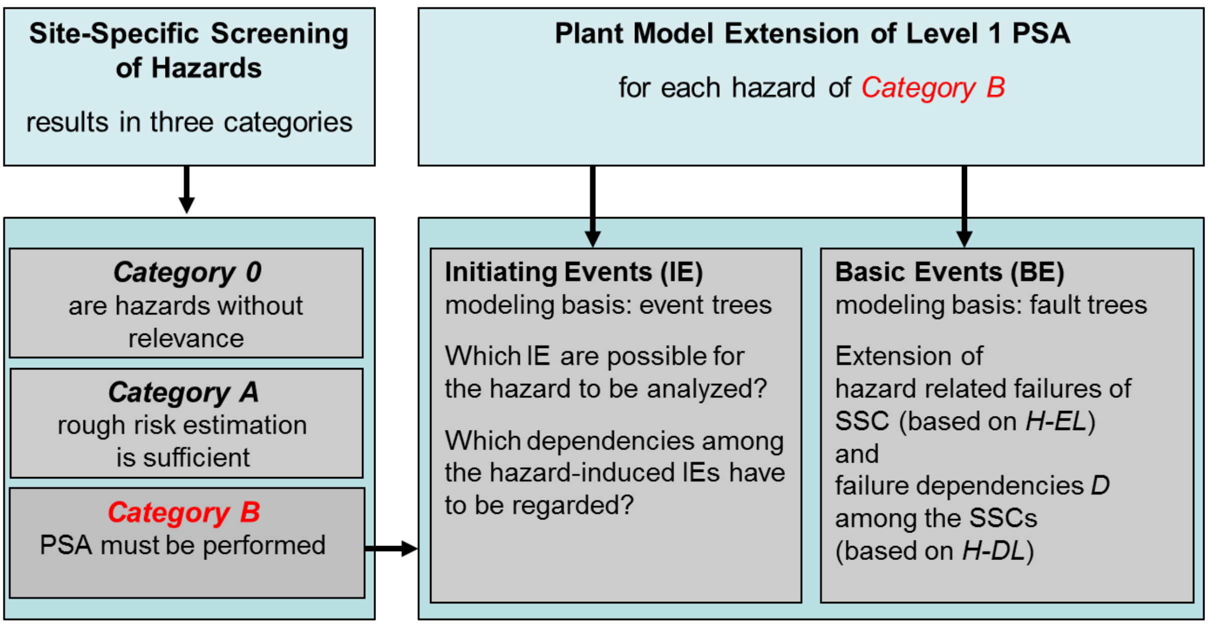


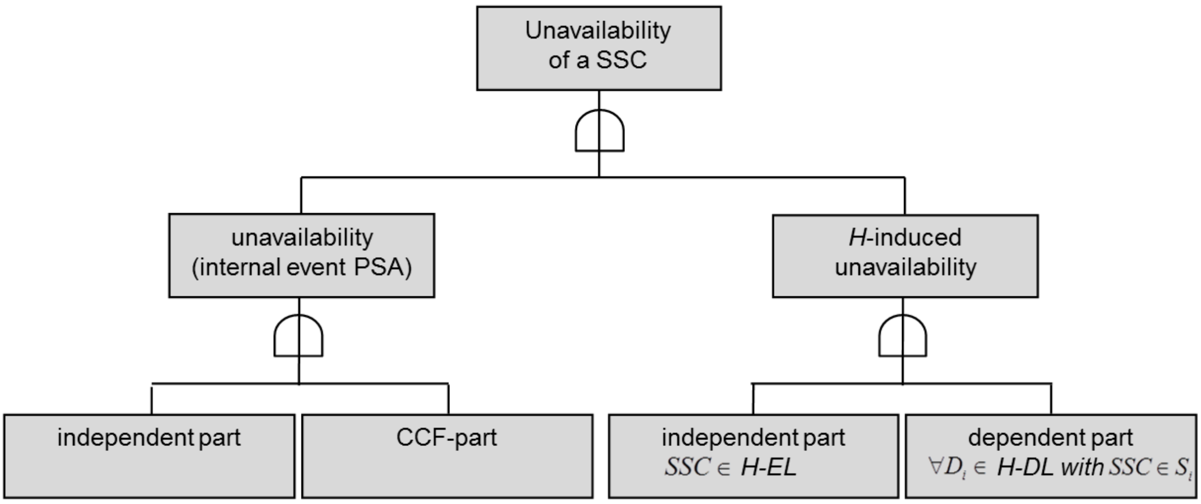
Figure 1: Structure of a Hazards PSA

On the first modeling level, it has to be analyzed which hazards and which combinations of hazards are relevant at the NPP site under inevestigation, that is to decide which of the hazards may contribute to the risk and which of them can be neglected in the further modeling. The second and third modeling level of an HPSA are performed for each relevant hazard and hazard combination identified on the first modeling level. The second modeling level is concerned with the induced initiating events by the relevant hazard. Thereby it is particularly important to examine whether the identified initiating events must be modeled as so-called common cause initiators and to what extent the hazard induced initiating events occur simultaneously or nearly simultaneously. Such initiators have to be identified and to be included properly into the PSA model. The third level of modeling dealing with the hazard induced unavailabilities of structures, systems and components (SSC) is of particular interest. The plant risk model at hand must be extended to include hazard induced failures or unavailabilities. This extension is systematically undertaken based on the equipment and dependency lists *H-EL* and *H-DL,* which have been derived before.

The list *H-EL* includes all SSC that might fail and contribute to the overall risk in the event of hazard *H*. Starting from all SSC of a NPP, the identification of SSC that might fail due to the hazard starts by means of a qualitative screening process. A quantitative screening follows, thereby it is to decide, for which SSC a detailed determination of the hazard induced failure probability is actually necessary.

Any hazard related dependency of failure behavior between more than one SSC is characterized by a triple called *D*; *D = (A, S, c)*. *S* symbolizes the set of SSC which are assumed to fail dependently in case of a hazard. The symbol *A* denotes the common attribute of all SSC of *S* which may be responsible for more than one up to all SSC of *S* to fail in case of a hazard. The coupling function *c* describes to which extent the common attribute *A* causes failures of more than one SSC of *S* due to the hazard.
The list *H-DL* includes all dependencies *D* between SSC, which have to be considered in case of hazard induced failures. For the compilation of *H-DL*, a screening procedure is recommended. Both lists *H-EL* and *H-DL* are verified and supplemented in the course of extensive plant walkdowns.

If a SSC is an element of *H-EL* and if this SSC is also part of a dependency *D* from *H-DL*, the fault tree characterizing the unavailability of this SCC can be complemented as shown in Figure 2.



$$H\text{-}EL = \{SSC_1, SSC_2, \ldots, SSC_n\}$$
$$D\text{-}EL = \{D_1, D_2, \ldots, D_m\}\_with\_D_i = (A_i, S_i, c_i)\_i = 1, \ldots, m$$

Figure 2: Fault tree extension using *H-EL* und *H-DL*

This fault tree extension must be performed for all SSC from *H-EL* and for all dependencies *D* from *H-DL* with the SSC under consideration as an element of the corresponding dependency set *S*.

3 INTERNAL HAZARD FIRE

In the following, the systematic extension of a given PSA model is described in the event of the plant internal hazard fire. The fire equipment list *F-EL* and the fire dependency list *F-DL* are derived.

A licensee plans technical modifications with regard to the spent fuel pool cooling (cf. 3.1). A Level 1 PSA for internal events has provided the result that the risk (here: annual frequency of fuel damage states (FDF)) is smaller by factor 2 after the modifications. For approval by the regulatory authority, an improvement has to be proven also for hazards. In the following, the probabilistic analyses for the internal hazard fire are presented as part of the new HPSA approach. For the analyses it could be reverted to a Fire PSA for power operation (performed some years ago by GRS) and to the results of a Level 1 PSA (carried out by the licensee) comparing different alternatives of spent pool cooling.

3.1 Alternatives of spent pool cooling

Two alternatives of spent fuel pool cooling are outlined in Figure 3.

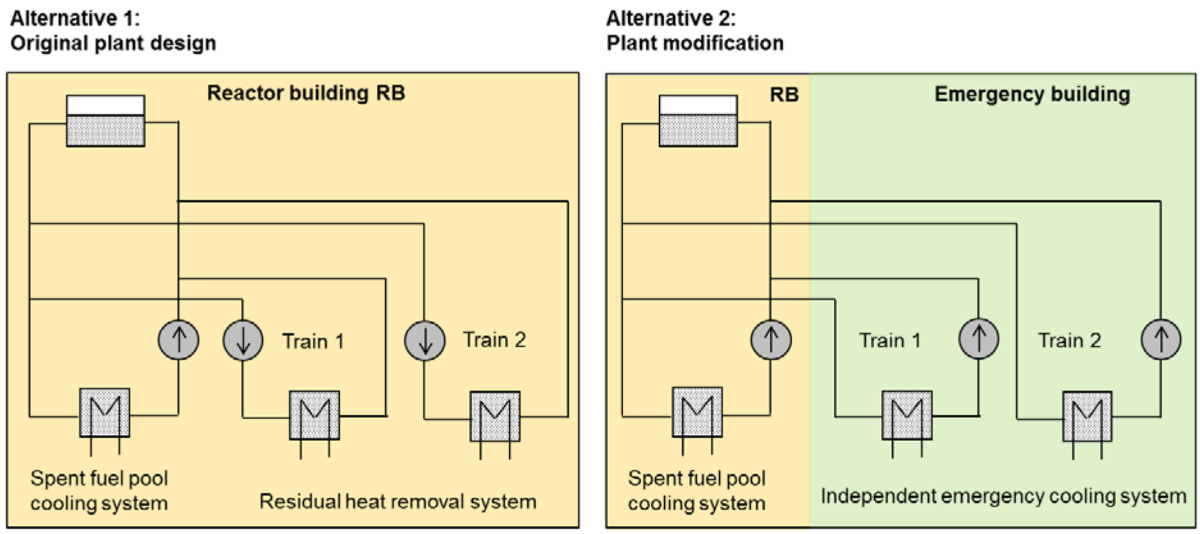


Figure 3: Alternatives of spent fuel pool cooling

In case of both alternatives, the cooling is normally done by the spent fuel pool cooling (SFPC) system. In case of alternative 1, the residual heat removal (RHR) system takes over with two redundant trains, if the SFPC system is not available, either unintendently due to a failure or due to intended outage, e.g. for maintenance reasons. The main parts of the SFPC and the RHR system are located inside the reactor building. With respect to alternative 2, two redundant trains of the independent emergency cooling (IEC) system are used if the SFPC system is not available. The IEC system is located inside the emergency building. It is protected against external hazards (aircraft crash, explosion pressure (blast) waves) and has two independent ultimate heat sinks. The purpose of the planned plant modification is to allow the licensee to start with deconstruction and decommissioning activities in certain areas of the reactor building.

3.2 PSA plant model modification due to fire events

The licensee has carried out a probabilistic risk analysis for comparing two different alternatives of spent fuel pool cooling for the longer duration post-commercial shutdown phase. The comparison of the risk is based on the annual frequency of fuel element damage states (FDF) for both alternatives. The post-commercial shutdown plant state is sub-divided in plant operational states (POS) representing typical configurations of the safety system according to maintenance and repair work during a reference year. The probabilistic plant model contains the entire POS and has to be extended such that the fire induced risk can be quantified.

GRS has performed a Fire PSA for full power plant operation for the plant under consideration in the past. For developing the fire equipment list *F-EL* and the fire dependency list *F-DL* in the frame of the fire specific risk asssessment of the two alternatives of the fuel pool cooling information from the former analyses has been used and modified with respect to the specific conditions of the longer duration post-commercial shutdown state. Starting point of a fire risk analysis is the disjoint sub-division of the relevant buildings into compartments (partitioning according to the plant labeling system). The fire induced frequency of fuel element damage (FDF) for each alternative of spent fuel cooling is derived by adding up the compartment specific FDF for all potential fires and the entire compartments. For simplification it is conservatively assumed that in the event of fire in a given compartment and failure of all fire extinguishing means to come into effect the entire equipment including cables in the fire compartment is unavailable. The compartment specific fire induced failure probability is estimated as product of compartment fire occurrence frequency and extinguishing failure probability.

Excerpt from **Fire Equipment List *F-EL***

component	**room**	**remark**
K_1	R1	Component itself (e.g. motor valve)
K_1	R2	power cable
K_1	R3	control cable
K_1	R4	control cable
K_1	…	…
…	…	…
K_n	…	…

Excerpt from **Fire Dependency List *F-DL***

fire compartment	**adjacent compartment**	c_{ij}
…	…	…
R5	R2	c_{52}
…	…	…
…	…	…

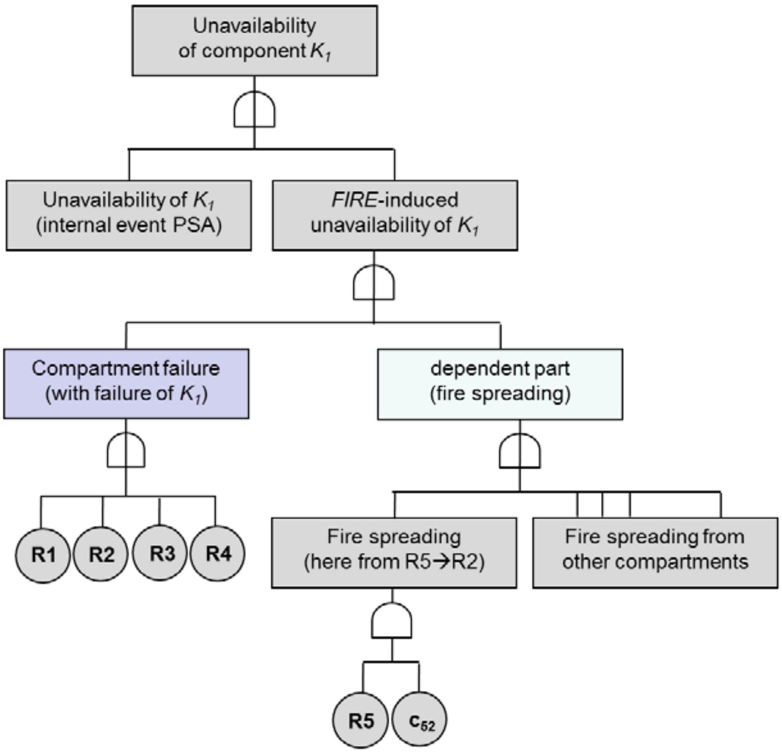


Figure 4: Fault tree extension using *F-EL* und *F-DL* in case of the internal hazard fire (exemplary component K_1)

Adopting information and data from the Fire PSA for power operation to low power and shutdown states it has to be checked if all the boundary conditions are still valid or have to be modified. Typically, changes are being observed with respect to the compartment specific fire loads. For the plant internal hazard fire, the equipment list *F-EL* contains a compartment-component assigment. Each component (including the corresponding cables) is assigned to a compartment. The overall unavailability of any component is estimated from its technical unavailability and the unavailability due to fire damage in those compartments, where the component or its cables are installed.

After derivation of the list *F-EL* the plant model can be systematically extended following the approach outlined in Figure 3 for any relevant component. In the example provided here, an automatic extension was carried out (cf. [5]). The list *F-EL* was generated supported by a database [7]. This database contains in particular the building partitioning including information on those compartments located directly adjacent to each compartment

(‘neighbouring compartments’), the corresponding fire barriers and the inventory of each compartment.
It is also possible to systematically consider fire propagation. In this context, the entire connections between any given fire compartment and its neighbouring ones (so-called compartment couples) are identified and stored in the list *F-DL*. A compartment couple (fire compartment and compartment to which the fire popagates) forms a set of dependencies *S*, *c* represents the conditional fire propagation probability. Only those compartments have to be considered, which contain components or corresponding cables relevant for the analysis.
As the list *F-DL* has been derived the plant model can be systematically extended applying the approch outlined in Figure 4 for each relevant component. For compartments containing relevant components those neighbouring compartments have to be identified, where a fire may occur and for which the probability of fire propagation to the compartment with the relevant component is non-negligble. In Figure 4, an incipient fire is possible to occur in the compartment R5 with the neighbouring compartment R1 containing the relevant comonent K1. The probability of fire propagation is c_{51}.
In the example of a probabilistic comparison of the two alternatives for the spent fuel pool cooling fire propagation could already be excluded at the beginning of the analyses.

3.3 Results

Comparing the two alternatives of the spent fuel pool cooling the following initiating events (IE) have been considered: loss of offsite power (LOP), failure of the residual heat removal (RHR) from the spent fuel pool, loss of water from the spent fuel pool, and flooding induced unavailability of the required system functions of the independent emergency systems (IES) building. Fires may cause the initiating events LOP and RHR failure from the spent fuel pool.
The quantitative anayses gave the result that the risk of fuel damage is much lower in case of the second alternative of spent fuel pool cooling.

It has to be mentioned in this context that the estimated risk values do not represent absolute values but should be only applied for comparison of the alternatives. For carrying out a Fire PSA for assessing the risk for the second alternative, the following steps should be performed in addition:

- Developing fault trees for the initiating events LOP and spent fuel pool RHR failure (in these fault trees the IE is traced back to fire induced component failures),
- Fire specific analyses for all POS of the post-commercial shutdown phase and the corresponding differences to power operation (compartment specific fire occurrence frequencies, possibilities of fire propagation, fire extinguishing possibilities, waiting periods extension).

Based on a full power operation Fire PSA and a comparative probabilistic analysis for plant internal initiating events, it was possble to carry out effectively and in a short time period a comparative fire risk analysis for two alternatives of spent fuel pool cooling in the frame of the more general HPSA approach.

4 CONCLUSIONS

After investigation of the reactor accidents at Fukushima Dai-ichi in March 2011 a systematic and as far as possible exhaustive conceptual approach is being developed to include all kinds of internal and external hazards into Level 1 PSA in a comprehensive manner. In this concept it is assumed that a comprehensive generic compilation (list) of hazards and possible hazard combinations is given. Within a site specific screening process it has to be decided how each hazard is to be assessed: the risk contribution of a given hazard can either be neglected, or the risk can be roughly assessed, or the risk must be calculated in detail by means of probabilistic methods.
A consistent approach for the requested extension of the plant model is proposed for all those hazards which must be analyzed in detail. For this purpose, lists of hazard relevant

SSC (*H-EL*) and their hazard related failure dependencies (*H-DL*) are derived in a systematic way.
Several parts of this conceptual approach have already been tested and practically applied.
In the paper, a successful application of the approach to the plant internal hazard fire is presented. A licensee plans a system modification of the spent fuel pool cooling, therefore a Level 1 PSA has been carried out to compare the fuel damage frequencies for both alternatives of spent fuel pool cooling, the original and the modified one. It has been outlined how the systematic (and partly automatic) extension of the fault trees is performed using the Fire Equipment List (*F-EL*). The *F-EL* contains a compartment assignment for all relevant components including cables. Furthermore, it is explained, how the possibility of fire propagation can be considered adequately using a Fire Dependency List (*F-DL*).
The probabilistic analysis of two alternatives of spent fuel pool cooling and a Fire PSA for power operation were used for a comparison of the two alternatives with respect to plant internal fires in the frame of a site specific hazard PSA approach.

5 REFERENCES

1. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU). Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes - Leitfaden Probabilistische Sicherheitsanalyse. Bekanntmachung vom 30. August 2005, Bundesanzeiger, Jahrgang 57, Nummer 207a, ISSN 0720-6100, Germany: 2005.
2. Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke. Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-358/05, Salzgitter, Germany: October 2005.
3. Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke. Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke,BfS-SCHR-38/05, Salzgitter, Germany: October 2005.
4. Türschmann M., et al. Verfahren zur Klassifizierung von Bauwerken, Systemen und Komponenten in Hinblick auf ihre sicherheitstechnische Bedeutung bei seismischen Einwirkungen. Technischer Fachbericht, GRS-A-3472, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Germany: 2010.
5. Herb, J. “Fault Tree Auto-Generator: How to Cope with Highly Redundant Systems”, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, (PSAM11 ESREL 2012). ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY: 2012.
6. Türschmann, M., S. Sperbeck, G. Thuma. “Recent Research on Natural Hazards PSA in Germany and Future Needs”, in: International workshop on PSA of natural external hazards including earthquakes, Prague, June 17-19th, 2013, to be published 2013.
7. Röwekamp, M., M. Türschmann, M. Schwarz, H.-P. Berg., “Database for a Comprehensive Fire PSA”, Paper 0113, in: Conference Proceedings of PSAM10 Conference, Seattle, WA, USA, June 2010.