Multinational Design Evaluation Programme

Technical Report

TR-VVERWG-10

Accident Management at Nuclear Power Plants with VVER Reactors

Countries involved in the MDEP working group discussions:	HAEA (Hungary), NNSA (People's Republic of China), Rostechnadzor (Russian Federation), NDK (Türkiye)
Countries which support the present Technical Report	HAEA (Hungary), NNSA (People's Republic of China), Rostechnadzor (Russian Federation), NDK (Türkiye)

Contents

List of figures and table

List of abbreviations and acronyms

BDBA	Beyond Design Basis Accidents
CSF	Critical Safety Functions
DBA	Design Basis Accidents
DEC-A	Design Extension Conditions Without Significant Core Damage
DEC-B	Design Extension Conditions with Core Melt
DiD	Defence in depth
EOP	Emergency Operating Procedures
IAEA	International Atomic Energy Agency
MCR	Main Control Room
SA	Severe Accident
SAR	Safety Analysis Report
TESG SA & AT	Technical Expert Subgroup Severe Accidents and Accident Transient

1. General view on accident management

The main objective of this report is to exchange experience and to compare the approaches and practical solutions adopted by regulators of the member countries in terms of accident management, including severe accident (SA) management. This report does not cover all aspects of accident management and is primarily devoted to regulatory requirements (criteria) applicable to assessing the operating organization's readiness to manage accidents, issues of developing emergency documentation and substantiating the effectiveness of accident management, as well as the role of the regulatory body in ensuring successful accident management.

Accident management plays a significant role in overall safety activities. In the structure of technical and organizational means ensuring defence in depth (DiD) at nuclear powerplants, accident management corresponds to the third and fourth levels. Table 1 shows two different approaches to structuring accident management activities. In one case (the far-left column), level 3 combines the management of design basis accidents (DBA) (3a) and the management of beyond design basis accidents (BDBA) without severe fuel damage (3b), while the management of beyond design basis accidents with severe fuel damage corresponds to level 4. The other approach is reflected in the far-right column, where the management of design basis accidents corresponds to level 3, and level 4 combines the management of accidents without severe fuel damage (4a) and the management of severe accidents (4b). This approach is adopted in Russia and China. Specifically, China considers design extension conditions without significant core damage (DEC-A) as 4a and design extension conditions with core melt (DEC-B) as 4b.

Table 1. Structure of DiD

Levels DiD Approach (1)	Objective	Technical means	Organizational means	Levels DiD Approach (2)
Level 1	Prevention of violation and failures	Conservative design, quality assurance	Instructions for normal operation and regulations	**Level 1**
Level 2	Operation with violation, indication of failures	Normal operation system. Protections for operation with violations	Instructions for operation with violations	**Level 2**
Level 3a	DBA Management	Safety systems	Emergency procedures for DBA	**Level 3**
Level 3b	BDBA management (prevention SA)	Technical means for BBDA management	Emergency procedures for BDBA	**Level 4a**
Level 4	BDBA management (mitigation the consequences of SA)	Technical means for SA management	Emergency instruction for SA	**Level 4b**
Level 5	Mitigation of radioactive consequences	Emergency response equipment	Emergency plan	**Level 5**

In accordance with the provisions of Russian and international regulatory documents, accident management activity covers level 3 and level 4 of DiD system implemented at the nuclear power plants.

To ensure accident management at the nuclear power plants, organizational measures must be implemented: development of procedures and guidelines containing instructions on accident management, training of personnel in skills for actions under accident conditions. The nuclear power plants design must provide for the presence of various technical means intended both for the prevention of BDBA (safety systems) and for mitigation of BDBA consequences (special technical means for BDBA managing).

Applicable requirement and regulations

Requirements for accident management at the nuclear power plants are installed in the following normative documents:

General Provisions for Safety Ensuring at of Nuclear Power Plants, NP-001-15 (pp. 1.2.11, 1.2.19, 3.1.3, 3.1.4, 3.1.5, 3.4.5.2, 4.1.5, 4.3.8, 4.3.9, 4.3.10);

Nuclear Safety Rules for Reactor Installations at Nuclear Power Plants, NP-082-07 (pp. 4.9, 4.10, 4.11, 4.12, 4.13).

Requirements for the content of Safety Analysis Report (SAR) for a nuclear power plant unit, NP-006-16

(p. 14.4.7).

Recommendations for the Structure and Content of the Guide to BDBA Management, Including Severe Accidents, RB-102-15;

Recommendations for the Development, Structure, and Content of the Instructions for Eliminating Design Basis Accidents at Nuclear Power Plants, RB-023-23;

Russian regulators also rely on the International Atomic Energy Agency (IAEA) requirements and recommendations:

- GSR Part 7 (Rev.1) Safety Assessment for Facilities and Activities, IAEA 2016
- SSR-2/2 (Rev/1) Safety of Nuclear Power Plants: Commissioning and Operation, IAEA. 2016 [3]
- SSG-54. Accident Management program for Nuclear Power Plants. Specific Safety Guides. IAEA. 2019.

China’s relevant regulatory bases are also consistent with the above IAEA requirements.

2. Structure and content of the accident management documentation

The development and commissioning of emergency documentation, as well as subsequent compliance with the instructions on the actions of personnel in emergency conditions, are ensured by the nuclear power plant administration on the basis of SAR and Technological Regulation. The structure of the emergency documentation is linked to the operating modes of the power unit. Transition from one level of accident management to another is defined by pre-established criterion presented in the accident management documentation. Figure 1 shows the relationship between operating modes and the structure of emergency documentation in accordance with the approach adopted at Russian nuclear power plants.

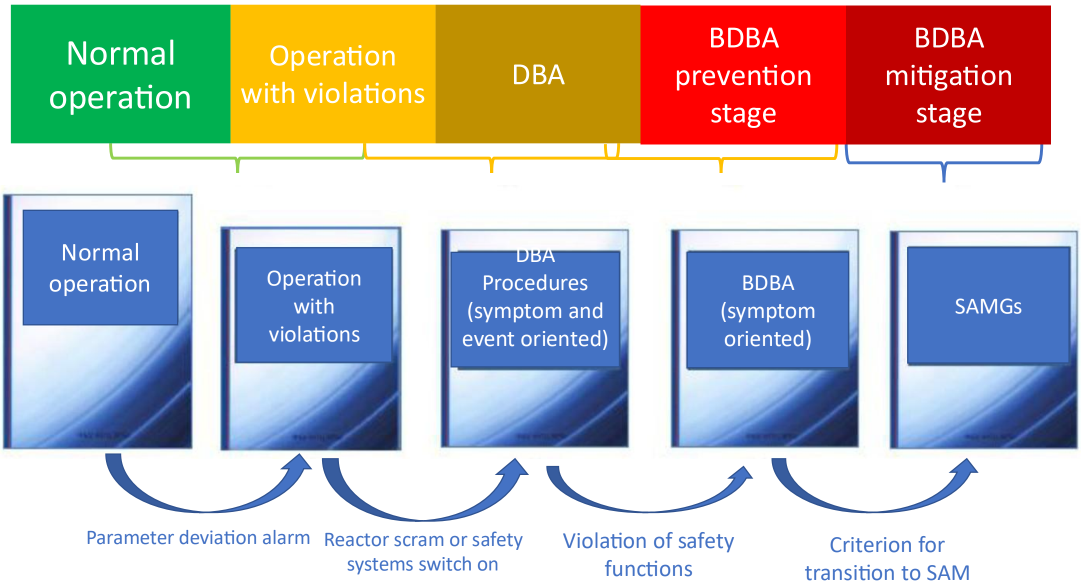

Figure 1. Operating modes and emergency documentation (ILA - procedures for DBA management (symptom and event oriented); RUZA -procedures for BDBA: RUZA (P) – prevention stage; RUZA (M) – mitigation stage

Normal operation of the nuclear power plants is carried out in accordance with the operating instructions. In the event that the parameters of the reactor plant deviate from the corresponding operating limits, alarms appear and the personnel act in accordance with the procedures 'Operation with violations' (response to signals). If the situation cannot be normalized and the change in the parameters of the reactor plant leads to the activation of the safety systems or the activation of the reactor emergency protection, the operating personnel proceed to perform actions in accordance with ILA procedures to prevent the escalation from DBA to BDBA.

In operational states with a shut-down reactor, the criterion for the transition to actions in accordance with the ILA procedures is the deviation of the monitored parameters from the operating limits established in the Technological Regulation.

At Russian nuclear power plants with VVER, two sets of ILA procedures are in effect simultaneously: a set of event-oriented procedures and a set of symptom-oriented procedures. The set of event-oriented procedures has priority. Application of event-oriented procedures implies identification of the initiating event. If it is not possible to identify the initial event, or if the actions in accordance with the event-oriented procedures are unsuccessful, the operating personnel shall proceed with actions according to symptom-oriented procedures. The actions according to the ILA procedures are terminated either in the case of successful achievement of the controlled safe state or in case if violation of the critical safety functions (CSF) occurs, the state of which is monitored from the beginning of the actions according to the ILA procedures. The state of the critical safety functions is displayed on special panels (safety parameter presentation panels) in the main control room.

In the case of violation of critical safety functions from the satisfactory state, the operating personnel cease actions in accordance with the ILA procedures and begin actions to restore critical safety functions defined in RUZA (P) procedures intended for prevention of severe accidents. Restoration of critical functions is carried out in accordance with the hierarchy of CSF, established in RUZA(P) from top to bottom in descending order of priority:

In the case of violation of critical safety functions from the satisfactory state, the operating personnel cease actions in accordance with the ILA procedures and begin actions to restore critical safety functions defined in RUZA (P) procedures intended for prevention of severe accidents. Restoration of critical functions is carried out in accordance with the hierarchy of CSF, established in RUZA(P) from top to bottom in descending order of priority:

- CSF-0: Equipment operability,
- CSF-1: Subcriticality of the core,
- CSF 2a: Cooling of nuclear fuel in the core,
- CSF -2b: Cooling of spent nuclear fuel in the spent fuel pool,
- CSF -3: Heat removal from the primary circuit to the secondary,
- CSF -4: Integrity of the primary circuit,
- CSF -5: Integrity of containment,
- CSF -6: Coolant reserve in the primary circuit.

For each critical function, the severity levels of its violation from satisfactory condition are defined, typically with 4 severity levels.

satisfactory condition: no actions are required to restore the CSF-1:

- **Unsatisfactory condition**: recovery actions are required, by decision of the emergency operations manager, the necessary actions are carried out either according to ILA procedures, or a transition is made to the recovery of the corresponding CSF according to RUZA (P) procedures.
- **Severe condition**: recovery actions are necessary, mandatory transition to actions to restore critical safety functions in accordance with RUZA (P) procedures is carried out.

- **Extreme condition**: immediate action is required to restore the CSF. For all CSF monitored in RUZA(P), violation criteria for each severity level, are defined and reflected in the state diagram (state tree) in Main Control Room (MCR).

The accident management actions provided for in the ILA procedures and the RUZA (P) procedures are aimed at preventing a severe accident. In many countries, these actions are combined in one document called "Emergency Operating Procedures (EOP)”.

All decisions at prevention stage of accident management are made by the emergency operations manager located at the MCR and are implemented by the operational personnel.

If severe fuel damage cannot be prevented and the criterion for transition to SA management, pre-established in RUZA (P), has been reached, the actions for CSF restoration are terminated and a decision to transition to severe accident management (i.e. actions in accordance with RUZA (M)) is made. At Russian nuclear power plants with VVER, the coolant temperature at the core outlet is adopted as a criterion for transition to SA management.

The importance of correctly defining the criterion for transition from the prevention to mitigation stage is determined by the fact that with the transition to mitigation stage, the priorities of actions for accident management change. If at the prevention stage, the priority was to prevent severe damage of the fuel (i.e. to preserve the reactor for future operation), then at the stage of mitigation the priority becomes maintaining the integrity of the containment and mitigation of the radioactive consequences of an accident.

The organization of accident management at the prevention stage differs significantly from that at the mitigation stage. At the prevention stage, actions on restoration of CSF are clearly defined in procedures, each of which corresponds to the severity level of CSF damage.

At mitigation stage, diagnostics of the reactor facility state are more complex and are carried out in two stages. At the first stage, in the order of pre-established priority, parameters are monitored whose deviation from the criteria indicates a serious threat to the integrity of the containment. Table 2 lists, in order of priority, the parameters are monitored at the first stage and a serious threat corresponding to them.

Table 2. Stage 1 monitoring parameters and corresponding serious threats

Monitored parameters	**Serios threats**
High activity out of the containment	Indication of untightening or bypass of the containment
High pressure in the containment	Threat of damage to the containment
High concentration of hydrogen in the containment	Threat of explosion of hydrogen-containing mixtures in the containment.
High level of vacuum in the containment	Threat of peeling of cladding in the containment

Each of serious threats listed has a corresponding mitigation strategy, presented in the instructions (ISU)[1]. If one of the serious threats is identified, the strategy presented in the corresponding instruction is implemented.

If no serious threats are identified, the second stage of diagnostics is carried out, during which the so-called "postponed threats" are identified (i.e. violation of monitored parameters from the pre-established criteria indicate a threat to integrity of the containment, which to the integrity of the containment. Table 2, in the order of priority established in the RUZA (T), lists the parameters whose monitoring is provided for at the second stage, as well as the corresponding postponed threats.

From a comparison of the parameters controlled at the first and second stages, it is clear that some parameters coincide, but the coinciding parameters have different priorities and different criteria for indication of threat.

[1] ISU is a short version инструкция серьезной угрозы in Latin alphabet. It can be translated as: Serious Threat Instructions.

Table 3. Stage 2 monitoring parameters and corresponding postponed threats

Monitored parameters	Postponed threat
Level in SG	Low SG level – risk of damage to heat exchange surface, possibility of containment bypass
Primary pressure	High pressure - risk of reactor damage at high pressure
Temperature at the outlet of the core	High temperature - risk of fuel damage
Temperature at the internal surface of the core catcher constructions	Temperature increase is indication of corium entering in the core catcher.
Activity out of containment	High activity – the evidence of containment bypass
Pressure in the containment	Risk of the containment damage
Concentration of hydrogen in the containment	Risk of explosion of hydrogen-containing mixtures in the containment

For each controlled parameter given in Table 3, the criteria are established, the violation of which indicates the need to go to the corresponding instruction of the RUZA (M) (ITA) to implement the strategy for mitigating the corresponding postponed threat. If no serious or postponed threats are identified, the achievement of achievement of a controlled safe state is monitored to terminate on SA management actions.

Decision-making procedure in SA management

At the mitigation stage of SA management, the assessment of the reactor facility state and implementation of the corresponding SA management strategy are the responsibility of the accident management group (AMG), which is specially created at the nuclear power plants and consists of several specialists with specialized knowledge and training in SA management.

In the case of postponed threat is indicated, the decision to implement the strategy is made on the basis of a) reactor plant diagnostics and b) on the comparative assessment of the negative and positive consequences from the strategy implementation. If, based on the results of the assessment, the negative consequences prevail over the benefits of the strategy implementation, it is possible to refuse the implementation of the strategy. In the case of severe threat is identified, actions provided in the relevant instructions (ISU) are carried out immediately, without assessing possible and negative consequences.

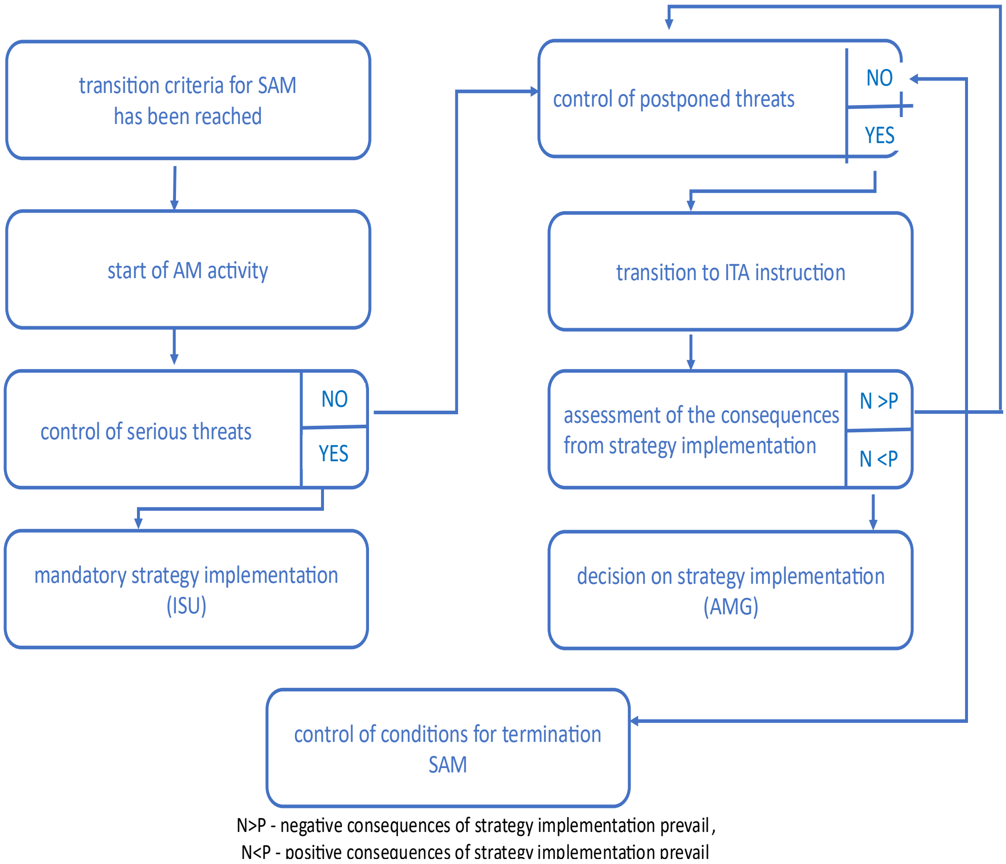

Figure 2. Decision-making scheme at the mitigation stage of the TA

3. Justification of the effectiveness of emergency procedures and instructions

In accordance with the approach adopted for Russian nuclear power plants, the efficiency of the procedures and instructions should be justified on the basis of deterministic analysis results. (requirement p.14.4.7 NP-006-16). It should be demonstrated that realization of accident management strategies provided in emergency procedures and instructions resulted in achieving a stable and safe state of the reactor facility, when the main critical safety functions (subcriticality, fuel cooling, localization of radioactivity) are fulfilled. At the same time, it must be confirmed that the technical and organizational means provided in the design for accident management ensure:

- integrity and tightness of the containment,

- elimination of hydrogen explosions,
- elimination of reactor vessel rupture under high pressure conditions.

4. Activities of the operating organization to ensure accident management at nuclear power plants

In an emergency, a clear distribution of duties and responsibilities plays an important role. Therefore, in the emergency documentation (ILA, RUZA), the duties and responsibilities of all participants in the accident management process must be clearly defined, while the level of responsibility for the decision taken must be commensurate with the complexity of the task and the potential consequences of those decisions. At the stage of preventing severe fuel damage, the main responsibility lies with the emergency manager. The decision on the choice of procedure and technical means is made by the head of emergency operations, usually the shift supervisor of the unit. At the stage of mitigating the consequences of SA, a larger number of factors must be considered when making decisions on the management of processes that, in some cases, have not been sufficiently studied, to have an understanding of the consequences of the decisions taken. For this, a specially trained accident management group is created. At some nuclear power plants, it is called the technical support centre. It is this group that assumes responsibility for assessing the state of the nuclear power plants and preparing decisions on the implementation of strategies.

The process of transition from one stage of accident management (prevention of accident) to another stage (mitigation of accident consequences) should be described in the RUZA (P) and in the RUZA (M), including the conditions for starting the work of the AMG (technical support centre). The process of preparation for the start of the work of the AMG (or technical support centre) takes time — time is needed to gather the AMG members, to inform all employees about the general situation, and to give them the opportunity to assess the state of the plant; only after that will they be ready to give their first recommendation on the implementation of the strategies provided in the RUZA (M) instructions.. The operating personnel should be ready to carry out initial actions on accident management until the AMG starts working. For this period, the relevant instructions should be provided in the RUZA (M). If during an accident the possibility of delegating authority for accident management actions within the operating organization is considered, it should be checked that the person to whom the authority will be delegated has the necessary experience to effectively exercise such authority.

The transfer of authority and responsibility in the accident management process should take place when risks to the safe and effective implementation of accident management strategies are minimal. The transfer of responsibility and authority should not result in delays in decision-making or the implementation of necessary actions. At the same time transfer of responsibility and authority should not take place until the new decision maker is ready to assume the responsibility.

The minimal necessary list of persons who will participate in accident management shall be established at the nuclear power plants. When compiling the list, it is necessary to consider the possibility of an accident developing over a long period of time, considering shift basis, nighttime and non-working days. At multi-unit sites, it is necessary to consider the possibility of an accident developing at all units simultaneously.

The personnel participating in accident management shall be appropriately trained. The levels of training of different groups of personnel shall correspond to their roles and responsibilities. The personnel responsible for the implementation of accident management measures shall have the skills and qualifications to handle technical means for accident management.

The personnel of the control room and the members of the emergency support team shall have their own training programs corresponding to the level of involvement in accident management. Decision makers must be trained to understand and analyse the consequences and uncertainties accompanying the decision taken, they must understand the processes and phenomena taking place and make decisions on this basis.

Training, including periodic drills and exercises, must be sufficiently representative and realistic to prepare accident management personnel to respond to potential situations. Drills must be long enough to ensure that all services are prepared to perform their duties beyond a single shift. Information transfer skills during personnel shifts at all levels of accident management must be specifically practiced.

Training should cover accidents occurring simultaneously at multiple nuclear power plant units, accidents occurring in various reactor operating modes, accidents in the spent fuel pool, and situations where the central control room's monitoring and control functions are unavailable.

The results of drills and exercises must be systematically evaluated to provide feedback for improving the training program and, where necessary, refining procedures and instructions.

Severe accident management at nuclear power plants operating or under construction requires the use of mobile equipment. This mobile equipment requires regular maintenance and personnel training to ensure its readiness and reliability.

5. The role of the regulatory body in ensuring successful accident management

In Russia, emergency documentation (procedures and instructions) is a mandatory part of the package of documents submitted by the licensee to obtain a license for operation of a power unit. Thus, the regulator makes a decision on issuing a license taking into account the results of the examination of instructions and procedures (including the calculation justification), thereby assessing the sufficiency of the technical and organizational measures provided by the Licensee for accident management.

The regulator takes part in personnel training and full-scale exercises as an observer, participates in the discussion of the results of exercises and training, presenting its comments and remarks, if any, thereby assessing the personnel training and readiness for accident management.

The regulator conducts inspections on the site, monitoring, among other things, the current state of emergency documentation and personnel training activities.

6. Conclusions

This report examines the fundamental principles of accident management, with a particular emphasis on severe accident management. Representatives of Technical Expert Subgroup Severe Accidents and Accident Transient (TESG SA & AT) member countries agreed that the fundamental principles for managing BDBA, including severe accidents, agreed upon by national regulatory bodies for nuclear power plants with VVER reactors are consistent with each other.