IAEA-EBP-WWER-12

XA0100422

ANTICIPATED TRANSIENTS WITHOUT SCRAM FOR WWER REACTORS

A PUBLICATION OF THE
EXTRABUDGETARY PROGRAMME ON
THE SAFETY OF WWER AND RBMK
NUCLEAR POWER PLANTS

December 1999

INTERNATIONAL ATOMIC ENERGY AGENCY

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

ANTICIPATED TRANSIENTS WITHOUT SCRAM FOR WWER REACTORS
IAEA, VIENNA, 1999
IAEA-EBP-WWER-12
ISSN 1025-2762

Printed by the IAEA in Austria
December 1999

FOREWORD

The IAEA initiated in 1990 a programme to assist the countries of central and eastern Europe and the former Soviet Union in evaluating the safety of their first generation WWER-440/230 nuclear power plants. The main objectives of the Programme were: to identify major design and operational safety issues; to establish international consensus on priorities for safety improvements; and to provide assistance in the review of the completeness and adequacy of safety improvement programmes.

The scope of the Programme was extended in 1992 to include RBMK, WWER-440/213 and WWER-1000 plants in operation and under construction. The Programme is complemented by national and regional technical co-operation projects.

The Programme is pursued by means of plant specific safety review missions to assess the adequacy of design and operational practices; Assessment of Safety Significant Events Team (ASSET) reviews of operational performance; reviews of plant design, including seismic safety studies; and topical meetings on generic safety issues. Other components are: follow-up safety missions to nuclear plants to check the status of implementation of IAEA recommendations; assessments of safety improvements implemented or proposed; peer reviews of safety studies, and training workshops. The IAEA is also maintaining a database on the technical safety issues identified for each plant and the status of implementation of safety improvements. An additional important element is the provision of assistance by the IAEA to strengthen regulatory authorities.

The Programme implementation depends on voluntary extrabudgetary contributions from IAEA Member States and on financial support from the IAEA Regular Budget and the Technical Co-operation Fund.

For the extrabudgetary part, a Steering Committee provides co-ordination and guidance to the IAEA on technical matters and serves as forum for exchange of information with the European Commission and with other international and financial organizations. The general scope and results of the Programme are reviewed at relevant Technical Co-operation and Advisory Group meetings.

The Programme, which takes into account the results of other relevant national, bilateral and multilateral activities, provides a forum to establish international consensus on the technical basis for upgrading the safety of WWER and RBMK nuclear power plants.

The IAEA further provides technical advice in the co-ordination structure established by the Group of 24 OECD countries through the European Commission to provide technical assistance on nuclear safety matters to the countries of central and eastern Europe and the former Soviet Union.

Results, recommendations and conclusions resulting from the IAEA Programme are intended only to assist national decision makers who have the sole responsibilities for the regulation and safe operation of their nuclear power plants. Moreover, they do not replace a comprehensive safety assessment which needs to be performed in the frame of the national licensing process.

EDITORIAL NOTE

CONTENTS

SUMMARY

Anticipated transients without scram (ATWS) are anticipated operational occurrences followed by the failure of one reactor scram function. Current international practice requires that the capability of pressurized water reactors (PWRs) to cope with ATWS be demonstrated following a systematic evaluation of plants' defence in depth. Countries operating PWRs require design consideration of ATWS events on a deterministic basis. The regulatory requirements may concern either specific mitigating systems or acceptable plant performance during these events. The prevailing international practice for performing transient analysis of ATWS for licensing is the best estimate approach.

Available transient analyses of ATWS events indicate that WWER reactors, like PWRs, have the tendency to shut themselves down if the inherent nuclear feedback is sufficiently negative. Various control and limitation functions of the WWER plants also provide a degree of defence against ATWS.

However, for most WWER plants, complete and systematic ATWS analyses have yet to be submitted for rigorous review by the regulatory authorities and preventive or mitigative measures have not been established. In addition, it has also been recognized that plant behaviour in case of ATWS also relies on certain system functions (use of pressurizer safety valves for liquid discharge, availability of steam dump valve to both the condenser (BRU-K) and the atmosphere (BRU-A) for secondary side pressure control, and others) which have been identified as safety issues and need to be qualified for accident conditions.

In all countries operating WWERs, the need for ATWS investigations is recognized and reflected in the safety improvement programmes. ATWS analysis for WWERs is not required for the licensing process in Bulgaria, the Czech Republic (with the exception of the Temelin nuclear power plant) and Russia. Design consideration of ATWS is required if expert assessments of probabilistic safety assessment (PSA) results show that the ATWS could contribute essentially to the probability of core damage or to off-site radioactive releases (Russia) or in cases where there is only one fast acting shutdown system for which the Regulatory Authority stipulates that failure must be assumed.

The development of a national policy on the ATWS issue in line with international practices is recommended for national regulatory authorities. This policy should consider the systems necessary to mitigate consequences and/or requirements for acceptable plant performance in an ATWS event.

This publication provides guidance on the performance of ATWS analyses of transients for licensing purposes, on the initiating events identified for those WWER reactors, and on the best estimate approach to the transient analysis of ATWS events. Further guidance is directed at reliability assessment of instrumentation and control (I&C) related to ATWS, including its common mode failure potential, and the qualification of systems and components necessary for operation under accident conditions to mitigate ATWS.

While focusing on WWER-1000 reactors, this publication also provides guidance for ATWS events in WWER-440 reactors, taking into consideration the differences of this reactor type and its I&C.

1. INTRODUCTION

The lack of results from analyses for ATWS at WWER-1000/320 plants has been identified as a safety issue for these plants [1]. No preventive or mitigative measures have been implemented at operating units specifically for ATWS events, although some existing systems might also be useful in ATWS events. Other safety issues related to ATWS events mentioned in Ref. [1] are, for example, the qualification of pressurizer safety valves for water flow. This situation is a deviation from international practice.

The lack of explicit ATWS rules concerning requirements on analysis and/or systems covering ATWS events in countries operating WWER reactors creates confusion as to what is an acceptable approach to resolving the ATWS issue. Therefore, with regard to the WWER-1000/320 and 440/213 plants, the prevailing international practices should be adopted.

A consultants meeting on "ATWS for WWER-1000 Reactors" was convened in Vienna in August 1996 [2]. The meeting was used as a forum for the exchange of international practices concerning the scope, assumptions, acceptance criteria, and methodology used for system transient analysis of ATWS events.

The objective of this publication is to provide assistance for assessing the ability of WWER reactors to cope with ATWS events. This assistance is provided as a guidance, rather than evaluations. This publication is mainly concerned with WWER-1000 reactors, but some features specific to WWER-440 reactors are also included when discussing ATWS scenarios. Western experiences on ATWS requirements and practices have been contributed by Finland, France, Germany, and the USA.

The publication is structured as follows:

Section 2 summarizes the safety rules and practices concerning ATWS in different countries.

Section 3 discusses various aspects of ATWS scenarios from initiating events to mitigating the consequences. This section is intended to support the understanding of issues. In addition, it addresses the defence in depth approach to ATWS assessment and the significant features of various scenarios.

Section 4 is devoted to providing guidance for performing specific ATWS analyses using computer codes. This guidance reflects international practice. ATWS events in PSA assessments are also considered. The role of generic ATWS analysis is highlighted.

Finally, Section 5 presents general conclusions.

2. SAFETY RULES AND PRACTICES FOR ATWS IN DIFFERENT COUNTRIES

2.1. BULGARIA

The list of initiating events to be analysed for plant licensing is defined in Annex 3 to Order No. 5 of the "Law on the Use of Atomic Energy for Peaceful Purposes". This list does not include ATWS. In addition, there is no direct requirement to consider ATWS events in the relevant Russian regulations applicable to WWER reactors.

Until now, no request has been issued by the Bulgarian Nuclear Safety Authority (BNSA) to the Kozloduy NPP for a demonstration of the plant's abilities to cope with such events. ATWS events are not considered in the Technical Specifications and in the emergency operating procedures. Some analyses have been performed at the Kozloduy NPP Unit 5 for the purposes of Level 1 PSA, such as loss of off-site power and medium break loss of control accident (LOCA) ($D_n = 200$ mm in the cold leg).

ATWS events are included in the event trees of the Kozloduy NPP Unit 3 Level 1 PSA study, which is currently under way.

2.2. CZECH REPUBLIC

In the Czech Republic, consideration of the ATWS related accidents is not required by the regulations as part of the Safety Analysis Report (SAR). Nevertheless, they were included into the Temelin NPP SAR prepared by Westinghouse, in compliance with the US regulatory requirements of the NUREG-0800 "Standard Review Plan".

A similar scope for ATWS calculations is recommended by the IAEA [3] and the European Nuclear Assistance Consortium (ENAC) [4].

Following these recommendations, the Nuclear Research Institute (NRI) in Řež has started ATWS calculations for WWER-440/213 NPPs, especially with regard to loss of feedwater and loss of flow in the core.

ATWS analyses have also been performed for the WWER-1000 plant using the RELAP5 computer code. The following accidents in particular were taken into account: loss of flow; inadvertent opening of the pressurizer safety valves; inadvertent opening of steam dump valves to the atmosphere; leakage from the pressurizer's upper part.

According to previous US practice, the ATWS related calculations should consider the following limiting values:

- fuel damage limits are not exceeded during ATWS events
- reactor coolant pressure boundary limits are not exceeded during ATWS events.

For Temelin NPP, a diverse protection system (DPS) was required, based on the assumption that a hypothetical common mode failure (CMF) in the hardware or software portions of the programmable primary reactor protection systems (PRPS) occurs simultaneously with any event judged more frequent than once every 1000 reactor years (this includes the reactor coolant system (RCS) and steam leaks). The DPS thus backs up the PRPS for reactor trip and for engineered safety features (ESF) actuation and control. The DPS verification analyses, together with ATWS analyses, have been provided to the regulatory authority.

2.3. FINLAND

The position of the Finnish Regulatory Authority STUK on ATWS requirements is presented in the Guides YVL 2.2. and YVL 2.4. The former concerns transient and accident analyses and the latter concerns overpressure protection. The basic approach is to consider ATWS events as design basis events. Therefore, the general assumptions and acceptance criteria for postulated accidents are also applied to ATWS events. This implies conservative assumptions regarding uncertainties in various parameters and system characteristics and, as a rule, safety systems are assumed to operate in their minimum design configuration. More explicit information can be found in the Appendix of Ref. [2].

The STUK Guides represent an acceptable approach and level of safety for the licensing of new nuclear plants. It should be noted that the requirements are performance requirements and do not stipulate which systems should be installed to achieve that performance. The approach is also deterministic.

Nevertheless, probabilistic arguments to exclude very low probability failure modes of reactor scram might still be acceptable if a sufficiently strong case is made. The requirements of the STUK Guides are also applied to operating units to the extent feasible during periodical analyses of their level of safety.

2.4. FRANCE

Two objectives are attached to ATWS event studies in the French approach:

- mitigate the consequences of the more penalizing initiating events such as loss of normal feedwater relative to the primary pressure criteria, and
- reduce the occurrence probability of ATWS events in French NPPs.

The outcomes of relevant studies have led to improvements by new and diverse actuation from low steam generator (SG) level such as turbine trip, emergency feedwater actuation and also reactor trip for plant series 1300 MW and particularly in the last designed N4 plants (1400 MW).

The French procedures for ATWS, the methodology and classification of events used and the improvements applied to all NPP categories from 900 MW to 1400 MW, are described in the Appendix of Ref. [2]. Basically, ATWS events are considered as belonging to the beyond design basis accidents (BDBA) category and are therefore studied with best estimate assumptions, fully in agreement with IAEA documentation [3].

All the category 2 initiating events (i.e. anticipated transients in IAEA definition) with ATWS conditions, are now required by the French safety authority for old plants (900 MW, 1300 MW) as well as for new ones (N4 plants).

2.5. GERMANY

The basic German Rules and Guidelines, the Safety Criteria of the Bundesministerium des Inneren (BMI) and the Guidelines of the Reaktor-Sicherheitskommission (RSK), require two independent and diverse shutdown systems. In addition, the activation signals for the protection system shall be redundant and derived from different process variables to achieve a high reliability of the fast scram function. Accessorily, Section 20 of the RSK Guidelines requires that an analysis of ATWS events be performed. A list of transients is specified and criteria for the availability of systems are given. All systems may be assumed to be functioning except those which are assumed to be disturbed. No additional single failure and no repair condition must be postulated. The acceptance criteria are to limit the maximum pressure loading of the primary circuit and to assure the functioning of the borating system and the heat removal system to bring the reactor to a long term subcritical condition. The requirements are listed in the Appendix of Ref. [2].

In practice the complete list of transients was analysed for a reference plant. The most challenging transients were analysed on a plant specific basis; the analysis is updated when changes in nuclear design or safety system functions are planned.

In addition to investigations required within the licensing process, the consequences of ATWS events assuming additional failures in safety functions were analysed in risk studies performed for German NPPs. These studies estimated the contribution of ATWS events to core damage frequency.

2.6. HUNGARY

In the original design there was no requirement to carry out analysis of ATWS events as part of the SAR. Therefore, the first ATWS analysis was performed in 1993 only in the framework of the AGNES project for the Paks NPP Unit 3.

According to the new regulations issued in 1997 there are regulatory requirements for ATWS events, stipulating that "the design basis shall also incorporate those anticipated operational occurrences which can be derived from the assumption that one of the safety protection functions will not work". The ATWS events have to be analysed whenever the frequency of the initiating event together with that of failure of any of the safety protection functions is higher than 10^{-5}/reactor-year.

These requirements have also been applied for the Periodic Safety Review of Paks NPP Units 1-2, which was completed in 1996. Numerical criteria for fuel elements as well as for primary and secondary circuit pressures have been established for ATWS analysis.

Best estimate calculations using the SMATRA code (developed by VTT, Finland) have been carried out for the following initiating events:

- inadvertent withdrawal of a control rod assembly group
- loss of feedwater
- loss of off-site power
- trip of both turbines
- inadvertent closure of the main steam isolation valve.

It was stated that in the course of the ATWS events analysed, no violation of safety criteria occurred. It was stated that neither the cladding temperatures nor the pressures exceed values allowed by the rules.

The new Hungarian regulations require updating the FSARs of the Paks units for the first time before the end of 2000, then continuously thereafter.

2.7. RUSSIAN FEDERATION

The ATWS concept is not mentioned in Russian regulations, and ATWS events are not included in the list of initiating events recommended by the Russian Safety Authority Gosatomnadzor for consideration in a WWER design. In other words, Gosatomnadzor does not bring up the deterministic requirement on the necessity of ATWS consideration.

The Russian safety rules indicate the safety goals which a reactor designer should try to attain: core melt frequency less than 10^{-5}/ reactor-year and excessive radioactivity release frequency, requiring the evacuation of the population, less than 10^{-7}/reactor-year. Therefore, all the initiating events which could contribute essentially to these values must be included (in accordance with OPB-88 [5]) in the BDBA list to be agreed upon with Gosatomnadzor and analysed.

However, reactor scram (AZ) failure is not included in the lists of BDBAs agreed upon with Gosatomnadzor for the Balakovo, Kalinin and Novovoronezh NPPs. The main reason for this fact is the low probability of reactor scram failure.

Nevertheless, ATWS scenarios for WWER-1000 reactors have been under detailed investigation in Russia since the beginning of the 1980s. The first studies were carried out in response to scientific interest or because of the development of the reactor designs for potential foreign customers. Many analyses of this type were performed in the framework of special governmental programmes usually established after serious incidents at operating plants, like TMI-2 or Chernobyl.

The qualitative analyses of many typical ATWS sequences indicated no violation of acceptance criteria used for design basis accidents (DBAs). As for the quantitative computer aided analyses, all the scenarios including a WWER reactor scram failure have been investigated up to now using a very conservative approach. In many studies, both the anticipated occurrences and some postulated accidents were taken as initiating events; the inoperability of favourable non-safety systems was assumed and the single failure principle was applied identically as for DBA analysis. For these studies, the worst NPP initial parameters (in terms of reactivity coefficients, core power distribution, reactor power, etc.) were selected as input data with errors and uncertainties.

2.8. SLOVAKIA

The ATWS related analysis was not originally considered within the framework of SARs until 1994.

Starting with the major gradual upgrading of Bohunice NPP Units 1 and 2 equipped with WWER-440/230 reactors, ATWS analyses were required by the Nuclear Regulatory Authority of the Slovak Republic to be included in the SAR for plant modifications.

The general regulatory requirement on accident analysis incorporating ATWS events was also issued in 1996. This requirement regarding conditions for ATWS analysis is consistent with the IAEA Guidelines [3]. The acceptance criteria for ATWS events were selected as for postulated accident conditions, with the exception of increased values for limitation of pressure both in the primary and secondary circuits.

Further restrictions were prescribed in 1997 under the preparatory phase of the SAR for the Mochovce NPP. Conditions for long term stable cooling of the reactor core are required if the departure from nuclear boiling ratio (DNBR) limit is exceeded.

Calculations were performed using realistic values of initial steady state parameters for RELAP5 and DYN3D best estimate codes. Except for the blocking of all control rods, all safety related equipment was assumed operable.

2.9. UKRAINE

According to the Ukrainian Law "On the Use of Nuclear Power and Radiation Safety" all power units have to obtain the license for operation before 2000. A new regulatory document: "The Requirements for Contents of Safety Analysis Report" was introduced in Ukraine in 1996.

One of the sections of the SAR deals with "ATWS analysis". The list of accidents and ATWS events has to be approved by the Nuclear Regulatory Administration.

In accordance with regulatory requirements, the utilities have to perform ATWS analyses and to define the probabilities of the transients.

Depending on the probability of ATWS events the following cases are to be evaluated:

(a) If ATWS events have not been considered in the original design, but have a high probability of occurrence, then they should be assessed according to DBA requirements. Based on the results of the assessment, procedures or system and component modifications should be implemented (e.g. replacement of pressurizer safety valves, using "feed and bleed" procedure).

(b) If ATWS events have not been considered in the original design, but have a low probability of occurrence ($<10^{-4}$/reactor-year) they can be analysed with less conservative assumption or best estimate methods.

(c) ATWS events with rather low probability ($<10^{-5}$/reactor-year) are not to be considered in the design, but may be studied from the accident management point of view.

2.10. UNITED STATES OF AMERICA

Current US regulatory requirements for operating plants

US Regulation 10 CFR-50.62 requires certain equipment modifications depending on the vendor, and requires no additional ATWS analyses.

- All PWRs must install a ATWS Mitigation Actuation System (AMSAC), diverse and independent from the reactor protection system, to automatically initiate auxiliary feedwater and turbine trip. This system is not required to meet safety system design criteria, and does not need to be redundant.
- All PWRs manufactured by Combustion Engineering or by Babcock and Wilcox must install a diverse scram system from the sensor to the interruption of power to the control rods. The diverse scram system may use output signals from sensors used in the reactor protection system. (The Nuclear Regulatory Commission (NRC) recognized that sensor CMFs were not potential causes of ATWS events because of the extensive functional diversity provided in PWR protection systems.) The diverse scram system need not meet protection system design criteria or be redundant. Westinghouse PWRs were not required to install a diverse scram system because they had larger safety valves that limited overpressure during ATWS events.

Basis for US 10 CFR-50.62

The US rule for existing plants was based upon a large body of ATWS analyses, mostly done using best estimate (or realistic) methods, which credited operational systems.

The homogeneous equilibrium model was applied for pressurizer safety valve liquid release.

Current US regulatory requirements for new plants

In 1993, the NRC issued the policy for technical and licensing issues on evolutionary and innovative reactors. Four points establishing requirements for protection of digital instrumentation and control systems were included in the policy against CMFs:

1. The applicant must assess defence in depth and diversity to demonstrate that the CMFs have been adequately addressed.

2. The applicant shall analyse each postulated CMF for each accident evaluated in the SAR using best-estimate methods, and demonstrate that adequate diversity exists.

3. If a postulated CMF could disable a safety function, then a diverse means unlikely to be disabled by the same CMF is required to perform the same or comparable function. The diverse function may be done by a non-safety system.

4. Safety grade controls and displays, independent and diverse from the safety grade computer, shall be provided in the control room for manual, system-level actuation of critical safety functions.

(**Authors' note**: The preceding underlined text is printed as such in the NRC document, indicating the areas where NRC commissioners overruled NRC staff.)

2.11. COMPARISON OF ATWS APPROACHES

It is possible to distinguish the following approaches to ATWS events that exist in different countries (as shown in Table I):

- Design consideration of ATWS events is required on a deterministic basis in some countries including USA, France, Germany, Finland, Slovakia, the Czech Republic for Temelin WWER-1000, and recently in Ukraine.

- ATWS analysis is not required for the licensing process in some countries including Bulgaria, the Czech Republic (with the exception of Temelin WWER-1000), and Russia.
- Design consideration of ATWS events is required, if expert judgements or PSA results show that ATWS events could contribute essentially to the probability of core damage or to off-site radioactivity release (Russia) or in cases where only one fast acting shutdown system exists for which the regulatory body stipulates that failure must be assumed.

In all countries operating WWER plants, the need for ATWS investigations is recognized and reflected in the safety improvement programmes.

In certain countries slightly different initial and boundary conditions and assumptions are used for system transient ATWS analysis.

- The regulatory body of Finland requires ATWS analyses which use DBA assumptions such as operation of a minimal set of safety systems and allowances for uncertainties (taking into account the single failure criterion). The same approach was accepted up to now in Russian design and scientific organization.

In all other countries, the best estimate approach to analysing ATWS was or is applied, namely:

- The operation of the normal operation systems including the control system is assumed possible, if their failure due to initiating events has a low probability.
- The best estimated values (realistic values) of initial parameters are used.
- The single failure criterion is not applied.

As deterministic safety acceptance criteria for ATWS are (or were) used, the criteria for postulated accidents (Finland, Russia) have to be applied, except that the admissible stresses must be in accordance with ASME Service Level C [6] (USA, Germany, Finland, France).

TABLE I. OVERVIEW OF SAFETY RULES AND PRACTICES FOR ATWS

Country	Regulatory requirements for licensing	Approach to ATWS Analysis	Analysed reactor types
Bulgaria	No direct requirements	Best estimate	WWER-440/230
			WWER-1000/320
Czech Republic	No direct requirements	Best estimate	WWER-440/213
	Yes	Best estimate	WWER-1000 Temelin NPP
Finland	Yes	Conservative	WWER-440/213
			WWER-1000/model 91
France	Yes	Best estimate	PWR-900
	Yes	Best estimate	PWR-1300
	Yes	Best estimate	N4
Germany	Yes	Best estimate	PWR
Hungary	Yes	Best estimate	WWER-440/213
Russia	No direct requirements	Conservative	WWER-440/all models
			WWER-1000/all models
Slovakia	Yes	Best estimate	WWER-440/230
			WWER-440/213
Ukraine	Yes	Conservative or best estimate depending on probability	WWER-440/213
			WWER-1000/320, 302, 338
USA	Yes	Best estimate	existing PWRs
	Yes	Best estimate	advanced reactors

3. PRINCIPLES FOR ATWS ASSESSMENT — ATWS SCENARIOS

The purpose of this section is to describe the principles which have been applied in western practices regarding ATWS which should be taken into account for establishing the guidance set forth in Section 4.

These principles are derived from the fundamental objective of ATWS events: the assessment of defence in depth. Although careful attention is paid to each level of defence, oversights (mistakes) may still occur. Therefore, the possibility that each level of defence can fail should be considered and the consequences determined for the dual purpose of judging its importance (and the depth to which its reliability should be evaluated), and the value of additional defence should it fail.

Initial ATWS assessment is a form of limited defence in depth assessment and should not be confused with licensing requirements or design criteria. Rules for protection against ATWS events have been established in western countries after the initial assessments were made. In some countries the rules for ATWS events prescribed design-specific modifications. In other countries the rules specified that the design meets certain ATWS analysis acceptance criteria. Establishing such rules is the decision of individual countries, and should come only after an evaluation of the ATWS risk.

Partial failures of scram, i.e. failure of more than one rod to be inserted within the design limit or fully inserted following scram, have been experienced in some WWER-1000 reactors and in some western PWRs. The direct and root causes of such partial failures have been identified and are being eliminated.

Scram failures of this type should be addressed by deterministic analyses as part of design basis events. A reasonable limit for the minimum number of control rods to be inserted should be established based on actual experience. Analyses should also consider (i.e. give credit to) any mitigating or compensatory measure taken to compensate for failures to fully insert control rods. PSA can be used to confirm that, as a result of the actions taken, core damage frequency is not significantly degraded. In such analyses, particular attention should be devoted to the consideration of steam line break accidents since multiple failure of the control rods to be fully inserted on scram actuation appears to have the greatest impact on this type of event. [7]

3.1. INITIATING EVENTS

For complete failure of scram, i.e. the inability to automatically drop control rods into the core, all "anticipated transients" should be assessed. These transients are defined as unscheduled events whose occurrence is expected during the plant lifetime (frequency of 10^{-2} events per reactor-year or higher).

Grouping of initiating events can be based on the expected phenomena following a complete failure of the control rods to drop into the core. Concerning the challenge to the barriers to fission product release, the following groups of events may be defined:

1. Transients which cause a rapid decrease in the core flow to power ratio, and as a consequence, possible boiling crisis and leading to fuel and cladding damage. This includes control rod withdrawal and loss of flow events.

2. Transients resulting in a rapid reduction in SG heat removal. These events include turbine trip, turbine load reduction and loss of main feedwater. The events cause rapid pressurization, opening of the pressurizer safety valves and, as a consequence, a decrease of primary coolant inventory. Initial reactor shutdown occurs by reactivity feedback due to an increase in moderator temperature and a decrease in moderator density.

For WWER-1000 NPPs, the loss of feedwater (including variations such as loss of condenser vacuum) deserves the most attention because it leads to an association of very severe challenges to the fuel rods (because the main coolant pumps (MCPs) are tripped on low SG water level) as well as to the pressure boundary.

These events have been identified as the most limiting ATWS events in PWRs of western design. Although the WWER-1000 reactors will have a significantly different response to loss of feedwater than western PWRs due to MCP trip on low SG level and the characteristics of horizontal SGs, similar consequences can also be expected. These events are difficult for computer calculations with respect to processes in the SG (heat transfer during simultaneous dryout and flow coastdown) and in the core (large power shape changes will occur as relative power shifts to the bottom of the core).

Turbine trip should also receive adequate attention due to its relatively high frequency and the fact that it bounds the turbine load reduction and loss of electric load.

3. Transients resulting from an increase of heat removal by the secondary side, such as, inadvertent opening of the BRU-K with a strongly negative moderator temperature coefficient (MTC). The number of BRU-K that might open due to a single instrument failure, considered as an "anticipated transient", should be specified. Most western plants are designed in such a way that a single instrument failure will not open more than one valve, and consider only a single inadvertent valve opening as an anticipated transient. These transients insert reactivity due to cooldown, and cause higher power generation and change in the power shape. In this case, core damage is the primary concern.

If only one steam valve can open for any failure classified as an anticipated transient, then the maximum power increase is limited to about 15%. If the feedwater pumps can match the steam flow, this event can generally be shown to require no protection. If the feedwater pumps cannot match the steam flow, then SG water level will decrease to the MCP trip set point. The resulting transient would be bounded by the loss of feedwater transient discussed above.

This class of events also includes turbine control malfunction during low power operation, causing the turbine steam load to increase to its maximum value (e.g. from 40% to 105%). These conditions need to be addressed because the power distribution may be more adverse than for transients starting at full power.

Some initiating events do not normally generate a scram signal unless there is a failure of the limitation system, but may still be ATWS initiators if all or part of the control rods fail to insert due to a mechanical failure. Such events include turbine trip (required power reduction to 40%), trip of two MCPs (40% or 50%), trip of one main feedwater pump (50%). These events can also be bounded by considering complete loss of reactor coolant flow (all four MCPs), or complete loss of feedwater flow.

3.2. SCRAM FAILURE MODES

Scram failure modes should be specified based on reliability evaluation that includes the reactor scram system and all other I&C systems that might be used to mitigate an ATWS event or recover from it. The purpose of this reliability assessment is not only to provide insights into the reliability of the reactor scram system, but also to judge independence/diversity vs. susceptibility to CMFs of other systems.

Although CMF rates are very complicated from the point of view of statistical quantification (since they are characterized by oversights in design, manufacture, maintenance, etc.), a systematic reliability assessment provides insight into their potential causes. Various methods exist for assigning CMF failure rates (e.g. beta, multiple Greek letter, etc.). Application of these methods is useful in determining the degree of independence of other systems.

Failure to scram can be caused by CMF in different parts of the reactor protection system, as follows:

1. The detection level for safety parameters, including the sensor and sensing (impulse) line. WWER-1000 NPPs, like western PWRs, have several scram functions. It is unlikely that failure of any one scram function (e.g. wide range SG level) could constitute an ATWS event. Therefore adequate defence against this type of failure probably exists that still requires

further investigation. If necessary, this issue can be investigated by analysing the response to an anticipated transient assuming failure for each individual signal into the protection system (with all other signals functioning).

2. Other electrical parts of the reactor trip system, including: signal conditioning or analog-to-digital conversion; digital processor (if applicable); comparators (bistables); voting logic (relays or solid-state); and scram breakers. These components may or may not be independent of other systems which would also mitigate an ATWS event. CMF of scram breakers has been cited in some studies as a weak point in scram reliability in western PWRs. This failure may not be a problem for WWER-1000 NPPs due to the preventive protection or limitation system (PZ) if it is shown that scram breaker failure, with all the PZ working properly, meets the acceptance criteria.

In such an assessment, either no credit should be given to MCP trip (unless it aggravates the event), or justification should be provided that the MCP breakers are unlikely to be affected by the same CMF that fails the scram breakers.

3. Mechanical parts, including control rod drive mechanisms and control rods themselves. Common mode failures that can cause both the mechanical failure of the control rod drive mechanisms or insertion of the control rods and also failure of other systems need not be considered. All other systems would perform with their normal reliability (unless impacted by the course of the ATWS event). All ATWS events initiated by loss of off-site power are in this category, i.e. only a mechanical failure can prevent control rod insertion if normal AC power is lost.

Availability of other control, limitation, and safety systems for CMF in the electrical parts of the scram system should be considered in accordance with the results of the reliability assessment.

For the mechanical failures mentioned above, no control rod insertion should be assumed in the ATWS analysis. All other systems can be considered to work normally.

3.3. ROLE OF CONTROL AND LIMITATION SYSTEMS

With respect to the availability of systems, the following should be considered for ATWS analysis:

- PZ for normal operation may be assumed to function normally, provided that:
  - it is not vulnerable to the same CMF that could defeat scram (the system designer/analyst must justify the independence), and
  - it is reliable and normally in service based on actual operating history.
- In the case of the mechanical failure mode, no control rod insertion whatsoever should be assumed.

The actuation of the following systems depends upon the initiating event, the postulated scram failure mode, and the insights gained from the reliability assessment (i.e. how susceptible is the system actuation to the same CMF that prevents scram?):

- Auxiliary and emergency feedwater.
- Turbine trip.
- MCP trip.

- Manual or automatic attempts to step rods in (via rod control system) would not be possible if the scram breakers are open, nor is it recommended for consideration for a hypothetical mechanical failure. Alternating up and down to step rods in is not a recommended immediate action to achieve plant shutdown.

3.4. REQUIRED SAFETY FUNCTIONS

All critical safety functions must be preserved following an ATWS event. These include RCS and containment integrity, reactivity for shutdown, RCS inventory control, decay heat removal and control of radioactive releases. The ability to cool down to cold shutdown must also be preserved. All countries have placed a high importance on the RCS peak pressure following an ATWS event because of the threat that RCS overpressure creates for these safety functions.

Ability to achieve stable hot shutdown and later cooldown includes:

- Availability of components needed for shutdown and for cooldown (e.g. boration and makeup systems),
- Functioning of instrumentation needed for cooldown (e.g. pressure and level transmitters exposed to RCS pressure), and
- Limited extent of fuel failures must not prevent normal plant cooldown.

The ATWS event challenges several safety functions such as primary circuit integrity (e.g. pressurizer safety valves), secondary side heat removal (feedwater supply and pressure relief), and shutdown (boration). Parametric studies are recommended to determine the minimum requirements for these functions to bring the plant to a safe final shutdown.

Such parametric studies are also very helpful for both PSA studies, and to determine the effectiveness of possible alternative ATWS mitigation features. This would include the effect of the moderator temperature coefficient (MTC), initial power level, time of operator action, as well as of additional failures.

3.5. MITIGATING MEASURES

The inherent feature that limits core power following an ATWS is a sufficiently negative reactivity feedback by the MTC. The effective negative reactivity feedback may be increased by manually or automatically tripping the turbine or the MCPs. These measures contribute to increasing the temperature in the primary circuit, thereby improving total reactivity feedback.

The activation of boron injection (e.g. high pressure boron injection system (TQn4), makeup system/boron solution tank (TK/TB)) will further reduce power. If the scram failure mode was not mechanical, insertion of control rods by other activation is also possible.

With respect to MTC (including possible very low MTC consideration), the use of a beginning of cycle (BOC) equilibrium xenon MTC is common practice, and typically bounds approximately 99% of core life for a baseload station.

Reduced power operation is often considered for operation with a very low MTC, and should therefore be covered by studies.

If operator action is taken into account, a case should be analysed considering no operator action until pseudo-steady-state conditions are reached in the RCS.

ATWS evaluations, independently reviewed, are an efficient tool for Member States to improve defence in depth against ATWS events. western countries have generally instituted rules requiring additional diversity in actuation of turbine trip, auxiliary or emergency feedwater, and in removing electric power from control rods. These functions also exist in WWER-1000 NPPs, but have not been designed with any intended degree of diversity in their actuation. For example, diverse actuation of limitation systems and MCP trip represent an additional defence. However, it should be noted that diversity may also have safety penalties such as dilution of training as well as of maintenance and management attention and design effort; diversity increases the complexity of design, operation and maintenance. Therefore, when considering new rules, the benefits of increased diversity should be properly weighed against the disadvantages.

As a defence against mechanical sticking of control rods or their drives, automation of the TQn4 boric acid safety system (or the TB and TK operational systems) could be considered. Since all protection signals may be assumed to exist for an ATWS event caused by mechanical failure of control rods, an ATWS signal could be generated by an observed failure to reduce neutron flux to less than some value (e.g. 5%) within a short time (e.g. 5 s) after any scram signal. The value of such automation is dependent upon the results of the ATWS evaluation which would include sensitivity to operator action time.

Requirements for boration of the primary circuit in an ATWS event can beconsidered in three phases:

1. Bringing the reactor to a stable condition with zero fission power.
2. Bringing the reactor to normal hot shutdown coolant conditions.
3. Bringing the reactor to cold shutdown coolant conditions.

The first phase is the actual mitigation phase of the ATWS event, i.e bringing the transient itself to an end by suppressing the fission power. If control rods cannot be moved at all, some boration of the primary circuit even slowly may be necessary to compensate for the reactivity effect from power reduction, if this cannot be accomplished by coolant temperature rise alone due to a low absolute value of the coolant temperature coefficient. This is as far as dynamic system simulations are usually carried out.

In order to reach the normal coolant temperature at hot shutdown, some additional boration may be required. If no control rods can be inserted, the total boron injection must compensate for the total power effect, must provide a subcriticality of at least one percent, and must ultimately compensate for the decay of xenon as well. It will typically take about 24 hours before xenon decays below its equilibrium concentration at full power. Before this time the xenon overshoot will in fact provide additional poisoning and subcriticality of the core.

To reach the cold shutdown state, two cases can be considered. First, if all control rods can be inserted into the core in the hot state, then early in the cycle it is typically possible (although not recommended) to maintain the reactor subcritical in cold conditions even without further addition of boron. Towards the end of cycle, as the MTC becomes larger, additional boration will become necessary. Second, if the control rods cannot be inserted into the core in the hot state, additional boration will be required even early in the cycle. The normal boron concentration requirement in the cold shutdown state will be sufficient in this case, since this concentration is set such that the reactor will remain subcritical even if all control rods are withdrawn from the core.

If the control rods cannot be inserted into the core in the cold state, higher than normal boron concentration will be required early in the cycle to achieve a subcriticality margin of 5% in reactivity for safe operations with an open reactor vessel.

3.6. QUALIFICATION OF SYSTEMS AND COMPONENTS

The following components or systems may be exposed to accident conditions different from their standard design conditions and therefore, special attention should be given to the qualification of these components for ATWS conditions:

- Pressurizer safety and relief valves and downstream piping for liquid relief: might valves fail in an open or partially open position? Would piping fail if all three safety valves opened with water relief?

- Emergency core cooling system (ECCS) and other RCS inventory control: will valves survive peak ATWS pressure?

- Instruments in RCS pressure boundary (pressure, level, flow, thermocouples): will they survive peak pressure? Instruments such as pressure, level, and flow instruments that are normally connected during hydrotest may need no additional qualification if their temperature is the same during hydrotest as during power operation.

- Steam generator integrity: will degradation in tubes or collectors that is tolerated or might exist during operation influence performance under peak ATWS pressure and temperature?

3.7. ATWS ISSUES REQUIRING SPECIAL ATTENTION

For many western PWRs, loss of feedwater is a likely consequence in many ATWS scenarios. In comparison, trip of MCPs is a likely consequence of many transients on WWER-1000 NPPs since MCPs would be tripped by containment isolation, low water level in the SGs, a steam line break signal, or loss of power. MCP trip has benefits to ATWS (by reducing core power), but may also have drawbacks. The following questions should be addressed in ATWS analyses:

1. What is the safety margin to core damage for loss of flow in all loops, especially at elevated core inlet temperatures?

2. What is the degree of independence between reactor trips and MCP trips? (Refer to Section 3.2 for assessment of independence as part of the reliability assessment.)

3. Following trip of all MCPs with low water level in the SGs, can natural circulation be maintained? Or will high void content in the reactor outlet and hot leg prevent natural circulation? If the latter occurs:

- Would the cessation of natural circulation cause RCS overpressurization? For example, even if the core is completely shut down, the volume expansion of boiling caused by decay heat alone would be a severe challenge to relieving capacity.

- For long term RCS heat extraction by the SG in the condensation mode, what is the potential for reactivity excursions caused by unborated water in the condensate that would collect in the SG cold leg?
  - Recovery procedures must be careful to ensure that an MCP is not restarted in a loop which may contain unborated water. (Do not restart MCP without hot leg subcooling and verification of natural circulation.)
  - The phenomena of restarting natural circulation when the RCS is refilled needs to be studied — but this is not unique to ATWS events. No established criteria for its assessment exist at present.

In this connection, it should be noted that the ATWS analyses available have shown that either single phase or two-phase natural circulation would exist in all ATWS scenarios in WWER-1000 NPPs during the time the MCPs are off. Loss of natural circulation is normally associated with situations in which the RCS inventory is insufficient to maintain liquid in the hot leg and the SG hot collector. Such a situation may not arise in any credible ATWS scenario in which the high pressure injection system (TQn3) is available. However, that tentative conclusion deserves further investigation.

4. How will the RCS pressure transient be affected by the transient heat transfer characteristics of the WWER-1000 horizontal SG during coincident dryout and reactor coolant flow coastdown in all loops? Heat transfer characteristics of a horizontal SG during simultaneous dryout and MCP coastdown deserve special study (separate component modelling and comparison with plant data is strongly recommended).

4. GUIDANCE FOR PERFORMING ATWS ANALYSES

4.1. INITIATING EVENTS

Definitions of ATWS can be found in a few regulatory documents which are in force at present (US 10 CFR, German RSK Guidelines, IAEA Guide 50-SG-D11, French Guidelines). According to these definitions, an ATWS event is an anticipated operational occurrence followed by the failure of the reactor scram function. Therefore, only the events which are expected once or several times during the life of the nuclear power unit must be considered as ATWS initiators. Such kinds of events are included in the list of WWER-1000 design basis events under the designation "violations of normal conditions of operation", which is considered to be equivalent to the western designation "anticipated operational occurrences".

For standard WWER-1000/320 NPPs, the conditions which are to be considered as potential ATWS transient initiators are listed below based on the recommendations set out in Ref. [3].

1. Inadvertent withdrawal of a control rod group during startup
2. Inadvertent withdrawal of a control rod group during power operation
3. Control rod (CR) maloperation:
   - drop of one CR
   - static misalignment of one CR in a group
4. Decrease of the boron concentration in the reactor coolant due to chemical and volume control system malfunction
5. Single and multiple MCP trips
6. Inadvertent actuation of ECCS during power operation
7. Chemical and volume control system malfunction that increases reactor coolant inventory
8. Feedwater system malfunctions that decrease feedwater temperature
9. Feedwater system malfunctions that increase feedwater flow rate
10. Secondary pressure regulator malfunctions that increase steam flow rate
11. Inadvertent opening of one steam generator safety or relief valve or turbine bypass valve
12. Control system malfunction that decreases steam flow rate
13. Loss of external electric load
14. Turbine stop valve closure
15. Main steam isolation valve closure

16. Loss of condenser vacuum
17. Main feedwater pump trips
18. Loss of on-site and off-site power to the station.

From the above list, only events such as turbine trip that are normally terminated by reactor scram (AZ) should be considered as potential candidates for the list of ATWS to be analysed.

The reactor protection system design for WWER-1000 plants has been developed with a view to reducing or limiting the reactor power and thereby avoiding an unnecessary reactor scram. There are four levels of reactor protection related to power reduction:

- *Preliminary protection of the second level (PZ-2 in the design documentation)*

  The function of PZ-2 is to stop the control rod group withdrawal to prevent a reactor power increase above the values allowed by the Technical Specifications.

- *Preliminary protection of the first level (PZ-1)*

  The function of PZ-1 is to insert the control rod groups (beginning with the "working" control group) with the normal velocity 2 cm/s to decrease the reactor power until the actuation signal disappears.

- *Accelerated off-loading of the unit (URB)*

  The function of URB is to decrease reactor power rapidly by means of preselected control rod group dropping (the power decrease depends upon the current worth of the preselected group). Further decreasing of the reactor power (if needed) up to the allowed level is performed by PZ-1 operation.

- *Emergency protection (AZ) which is the reactor trip portion of the protection system*

  The function of AZ is to decrease reactor power rapidly down to residual heat by means of the simultaneous dropping of all control rod groups, thereby bringing the core to subcriticality.

PZ and URB systems are designed as a whole based on the same principles applied for the reactor scram system. Typical signals and set points for PZ, URB and AZ actuation are listed in Table II to indicate the possible effect of these systems on the scenarios which may be important from the ATWS point of view. The list of signals and/or set point values may differ somewhat from plant to plant.

When considering the above list of occurrences and protection signals to find occurrences leading to reactor scram, one has to bear in mind that an ATWS event belongs to a category of events which should be handled differently from the DBA approach. In particular, with the exception of those systems which are affected by the initiating event itself or as a consequence thereof, all systems may be assumed to function as designed.

Therefore, the assumptions on the operability of PZ and URB systems have to be based on the scram failure modes assumed for the given ATWS analysis. Some failure modes may preclude the operation of PZ or/and URB (e.g. if mechanical sticking of control rods is assumed as the reason for the scram failure, URB must be assumed inoperable). Clearly, with this approach, the list of ATWS events to be analysed will be plant specific to some extent as certain PZ/URB set points and/or signals might vary from plant to plant.

TABLE II. WWER-1000 REACTOR PROTECTION SYSTEMS

Measured parameter	Condition for actuation
1. REACTOR TRIP (AZ)	
1.1. Period of neutron flux increase:	
in source range	< 10 s
in power range	< 10 s
1.2. Neutron power:	
in source range	variable set point
in power range	> 107% Nnom
1.3. Difference between saturation temperature in reactor and temperature in any hot leg	< 10°C
1.4. Pressurizer level	< 4.6 m
1.5. Coincidence of following signals:	
SG steamline pressure	< 4.9 MPa
Difference of saturation temperatures between primary system and any SG steamline	> 75°C
1.6. Fast decrease of MCP pressure difference	< 0.25 MPa
1.7. MCP loss of power:	
1 out of 2 MCPs, when	N>5% Nnom
2 out of 4 MCPs, when	N>75% Nnom
1.8. Coincidence of following signals:	
1.8.1. Pressure above core	< 14.7 MPa
Reactor power	> 75% Nnom
1.8.2. Coolant temperature in hot legs	> 260°C
Pressure above core	< 13.7 MPa
1.9. Pressure in any SG	> 7.8 MPa
1.10. Seismic activity high	
1.11. Level in any SG by operating MCP below Hnom	< -650 mm *
1.12. Frequency decrease on 3 out of 4 MCP power buses	< 46 Hz
1.13. Containment pressure	> 0.13 MPa
1.14. Primary system pressure	> 17.7 MPa
1.15. Coolant temperature in any hot leg above Tnom	> +8°C

* Note: Levels below nominal are normally indicated as negative.

TABLE II. (cont.)

Measured parameter	Condition for actuation
1.16. Push AZ button	
1.17. Loss of reactor protection system AC voltage	
1.18. Loss of reactor protection system DC voltage	
2. PREVENTIVE PROTECTION (PZ)	
2.1. PZ-1	
2.1.1. Period of neutron flux increase:	
in source range	< 20 s
in power range	< 20 s
2.1.2. Neutron power: in power range	> 104% Nnom
2.1.3. Reactor power too high for number of operating MCP or MFP	
4 MCPs in operation	> 102% Nnom
3 MCPs in operation	> 69% Nnom
2 MCPs in operation	> 42-52% Nnom
2 MFPs in operation	> 102% Nnom
1 MFP in operation	> 52% Nnom
0 MFP in operation	> 7% Nnom
2.1.4. Pressure above core	> 16.9 MPa
2.1.5. Coolant temperature in any hot leg above Tnom	> +3°C
2.1.6. Steam collector pressure	> 6.8 MPa
2.1.7. Frequency decrease on 3 out of 4 MCP power buses	< 49 Hz
2.1.8. Loss of MCP power — Reactor power limitation by ROM*	
1 out of 4 MCPs	> 75% Nnom
1 out of 3 MCPs	> 50% Nnom
2.1.9. Push PZ button	
2.2. PZ-2	
2.2.1. Neutron power in power range	> 101% Nnom
2.2.2. Pressure above core	> 16.2 MPa
2.2.3. Drop of any CR	

* Note: PZ-1 is actuated by ROM (power limitation controller) if the reactor power exceeds a limit that depends on the number of MCP remaining in operation. As a consequence, PZ-1 is deactuated (insertion of control rods stops) when power falls below the limit.

TABLE II. (cont.)

Measured parameter	Condition for actuation
2.2.4. Outlet temperature of any fuel assembly is high	
2.2.5. DNBR is low	
2.2.6. Local core power is high	
2.2.7. Reactor power for operating MCP number is high	
3. ACCELERATED UNIT OFF-LOADING (URB)	
3.1. Loss of power to 2 out of 4 MCPs	
3.2. Loss of power to 1 out of 2 MFPs	
3.3. Turbine trip	
3.4. Loss of external load	
3.5. Generator switch-off	

Nevertheless, to simplify the work on plant specific ATWS analysis and especially for the purposes of generic ATWS analysis, one may assume inoperability of all functions related to insertion of the control rods into the core. With this approach, it is recommended that the ATWS events listed in Ref. [8] be analysed for WWER-1000 nuclear power plants. These events are as follows:

1. Uncontrolled withdrawal of a control rod group during startup or power operation.
2. Loss of main feedwater flow.
3. Loss of on-site and off-site power to the station.
4. Loss of condenser vacuum.
5. Turbine trip.
6. Loss of electrical load.
7. Closure of main steam isolation valves.
8. Inadvertent opening of one steam generator safety or relief valve or turbine bypass valve.

4.2. ASSUMPTIONS

According to western practice, ATWS events belong to the BDBA category and can therefore be analysed with best estimate methods. The same approach should be applied for WWER-1000 reactors. Nevertheless, if the work performed in a particular country results in a relatively high probability of scram failure, the application of the best estimate method should be limited accordingly. The IAEA is currently developing a guidance which also includes the practical application of best estimate analysis.

The following sections present the main considerations on assumptions for best estimate analysis and set out some specific features relating to ATWS scenarios.

4.2.1. Initial conditions

Initial conditions (measured or calculated) should be chosen at their most probable values, without uncertainties and errors, and based on their operating range in the foreseen initial state. The initial conditions should be consistent at least for full load initial state. Of course, BOC or end of cycle (EOC) should be correspondingly chosen when penalizing for the considered event. Important parameters (reactivity coefficients, peaking factors, etc.) should correspond to the neutronic calculations without uncertainty and calculation errors. When calculating reactivity coefficients, equilibrium xenon at full power and xenon free at low power are to be assumed.

4.2.2. Operability of systems

Operability of systems should be considered in a realistic way.

- Proper modelling of all control and safety systems that affect the accident should be included. No failures, no artificial delay in the actuation signals, no conservative protection system set points, no penalizing value in the resulting effect should be considered in the analyses.

Non-safety systems or equipment may be considered and modelled in the analyses if they are designed to withstand the accident conditions. This covers particularly all the control devices, even when favourable consequences are foreseen. However, careful attention should be paid to the control system actuating a control rod group (temperature or power control rod group) as long as a clear understanding of independence between scram actuation signal and control actuation has not been established. In such a case, bearing in mind the CMF concept, it is recommended not to model the control function as a means for mitigating consequences of ATWS events.

Further applicable assumptions are as follows:

- The single failure assumption need not be considered, nor simultaneous repair work postulated.
- Loss of off-site power (LOOP) should not be considered unless it is a direct consequence of the initiating event or it is the initiating event itself.
- If the accident is affected by phenomena that cannot be modelled properly (e.g. due to the lack of the experimental data) an approach should be selected which derives conservative results.

4.2.3. Operator intervention

Provided there is a clear and reliable indication for diagnosis in the framework of ATWS events, the time for operator intervention may be assumed at a minimum of 10 minutes if the action can be initiated from the control room, when the action corresponds to the respective operating procedure and the operator has been adequately trained in its use. For other actions, this time margin should be evaluated in a realistic way.

4.3. ACCEPTANCE CRITERIA

In general, ATWS acceptance criteria are comparable to the criteria for postulated accidents (e.g. Appendix 2 of Ref. [3]) and address primary system integrity, fuel cooling capability, shutdown reactivity, and off-site radiological consequences. In particular:

1. International practice accepts less restrictive RCS pressure limits for ATWS. ATWS limits are generally based on allowable stress limits for ASME Service Level C or 135% of design pressure (for WWER-1000 reactors, this is also the primary circuit hydrotest pressure).

2. Fuel cooling capability should be demonstrated, i.e. core damage and calculated changes in core geometry do not prevent long term core cooling. However, there is no international consensus as to acceptance criteria. The following are examples of practices in Member States:

- In *Finland*, fuel and cladding temperatures and cladding oxidation are calculated in post DNB conditions if the minimum DNB ratio becomes less than the limit for anticipated transients. Safety factors accounting for uncertainties in fuel rod power and coolant conditions are applied to the hot fuel rod. The main acceptance criteria are 1200°C and 17% oxidation at the cladding hot spot. When estimating the number of fuel rods potentially in DNB, the uncertainty in fuel rod power is usually treated as a probability distribution.
- In *France*, cases are considered acceptable if the DNBR, calculated using best estimate methods, equals or exceeds the DNBR for anticipated transients, i.e. the value that gives 95% probability at the 95% confidence level that DNB does not occur. Cases with a lower DNBR can be considered probabilistically, if necessary, in conjunction with the variation of the moderator temperature coefficient during core life, to determine the fraction of cases in which DNB might occur. No such cases have been found to date. No attempt is made to calculate post-DNB fuel rod conditions. DNB during an ATWS event would be simply and conservatively assumed to be equivalent to core damage for the purposes of determining core damage frequency in the plant probabilistic safety analysis.
- In the *USA*, during the 1970s, a minimum DNBR of 1.00 or greater was advanced as a calculably convenient means of providing adequate assurance that no significant core damage would occur. Generic (best estimate) analyses reported significantly higher DNBRs. Subsequent adoption of 10CFR-50.62 focused further effort on ATWS mitigation and diverse protection rather than analyses (Section 2.9 of this publication). Current regulation and practice do not address either DNB or cladding temperatures for ATWS. Where assessments are done, analyses are limited to calculated peak RCS pressure.

3. The analysis of ATWS events should demonstrate that a safe and stable shutdown of the reactor is achieved. Common international practice is to accept a subcriticality of one percent as an adequate indication of reactor shutdown.

4. For radiological assessment, a generally accepted approach is to assume that fuel cladding failure (leakage) occurs for all fuel rods having a potential for boiling crisis, e.g. having a DNBR less than the value that gives 95% probability at 95% confidence level that DNB does not occur. Less conservative approaches have not been found necessary to demonstrate that site boundary limits for postulated accidents are not violated.

4.4. CODE AND MODELLING REQUIREMENTS

ATWS events are complex accidents which involve reactivity and power distribution anomalies in the core simultaneously with changing thermal and hydraulic conditions, such as:

- decrease in reactor flow rate
- decrease in reactor coolant inventory
- decrease or increase in heat removal by the secondary side.

Complex computer codes are needed for these analyses. The computer codes for the ATWS analysis must describe in sufficient detail all the main parts of the primary and secondary circuits of the nuclear power plant considered.

Moreover, bearing in mind the above assumptions, particular attention should be given to the following control functions:

- control systems of the primary circuit
  - pressurizer safety and relief valves
  - primary pressure control (pressurizer heaters and spray)

- pressurizer water level control (makeup and letdown)
- reactor power control.

- control systems of the secondary circuit
  - steam generator water level control (main and emergency feedwater)
  - safety valves
  - steam dump to the condenser
  - steam dump to the atmosphere
  - turbine control system.

Very important is the coupling of the neutron kinetics model with an adequate thermal-hydraulic model in the core. The following neutron kinetics models can be considered acceptable depending on the desired accuracy of the reactivity description and on the nature of the event:

Point kinetics model is available with some standard thermal-hydraulic system codes. Axial weighting when averaging the core thermal-hydraulic conditions for the point model is desirable to improve the feedback performance of the point model.

1D kinetics model is specifically intended for representing the axial core dimension in order to adapt to changing axial power shapes. The model will take properly into account the influence of possible strong changes in thermal-hydraulic conditions occurring along an (average) fuel assembly in the core, e.g. steam voids concentrating in the upper part of the core.

3D kinetics model is recommended for obtaining the best description of thermal-hydraulic feedback effects in the core. The model will properly account for the influence of different conditions in fuel assemblies with different powers, for the local influence of removing control rods from the core, for possible asymmetries in the core, etc. For symmetric transients, the model can be limited to a sector of the core.

Spatial kinetics models are needed in particular when steam is generated in the core or asymmetric conditions exist. A boron transport model is also needed.

Because steam can be produced in the core, a two-phase thermohydraulic model is needed in both the primary circuit and the secondary circuit. The six- or five-equation two-phase model is typically required.

All models and correlations used in the code should be documented. The applicability range of correlations must be stated and they should not be used outside that range.

The thermohydraulic correlations which are used should be verified for WWER conditions. Very important is the influence of the following correlations on the process :

- heat transfer correlations in the core
- discharge flow model of the safety valve of the pressurizer and the steam generator
- void fraction correlation on the secondary side of the steam generator.

Since the user of codes may not have been involved in the code development and testing, code documentation should include detailed user guidelines. These should include, among others, guidance on how to make a good nodalization scheme and detailed guidance in the use of each specific component, node type or separate model.

The nodalization of the following components have an important influence on the results of calculation:

- core
  - separate parallel channels
  - 3D kinetics model
- fuel rod
  - number of the nodes in the axial direction
  - number of the nodes in radial direction
- upper plenum and upper head
- down comer and lower plenum
- steam generator both on the primary and the secondary sides keeping in mind loss of feedwater accidents.

Advances in safety research usually lead to better understanding of physical phenomena and consequent improvements in the computer models. Each version of the code should be clearly identified and all corrections and changes clearly documented.

The requirements for code validation should follow Ref. [3]. The validation of nodalization schemes should be performed by comparing data from plant transients with code predictions.

4.5. APPLICATIONS OF ATWS ANALYSES

4.5.1. Generic

The major objective of generic analyses is to confirm that the plant is basically capable to cope with the defined ATWS events without exceeding acceptable limits. Due to this objective, the complete spectrum of the events mentioned in Section 4.1 has to be investigated for a representative plant using the assumptions mentioned.

Furthermore, the objectives of generic analyses are:

- to define the limiting events with respect to acceptance criteria
- to show the margins to the acceptance criteria
- to understand the basic physical phenomena to which the events are sensitive
- to find out which operational and protection systems are demanded during the transient
- to demonstrate that the actions of the demanded systems occur at the right moment and with the desired effect.

Parametric studies within these generic analyses may define the limiting values of the relevant parameters (e.g. reactivity feedback).

4.5.2. Plant specific analyses for licensing

For licensing purposes, the transients with small margins to acceptance criteria and in particular the limiting transients should be analysed with plant specific data using the same assumptions as used in the generic analysis.

For large margins to acceptance criteria, the need for specific analysis of the event may be reduced if it can be stated, taking into consideration the influence of differences in the design, that the results of the generic analyses are also basically valid for the specific plant.

4.5.3. ATWS analyses to support PSA studies

The objective of PSA studies is to determine the overall plant risk resulting from severe accidents. ATWS events imply overpressurization that may result in severe damage to the primary pressure boundary or direct severe damage in the core due to inadequate cooling.

The purpose of ATWS analyses to support PSA studies is to assess whether a given sequence of events indeed leads to severe damage. The assumptions in these analyses are not limited to those made for licensing purposes — multiple failures should be assumed.

On the other hand, results of PSA studies can provide feedback for analysing particular event sequences on a deterministic basis for licensing.

5. CONCLUSIONS

1. This publication deals primarily with WWER-1000 reactors. It also provides guidance for ATWS events in WWER-440 reactors, keeping in mind the differences of this reactor type and its I&C. A specific feature of the WWER-440 reactors regarding natural circulation is the presence of loop seals in the hot legs.

2. The fundamental objective of a complete ATWS evaluation is to assess defence in depth capabilities of NPPs relative to these events. The purpose is to assist in judging the adequacy of the reactor trip protection system and the value of additional defence should this fail. This publication is intended to assist in deciding what additional defence may be desirable.

3. In all the western countries represented in Ref. [2], design consideration of ATWS events is required on a deterministic basis. The regulatory requirements can concern either specific mitigating systems or acceptable plant performance during these events. The prevailing international practice for performing system transient analyses of ATWS events for licensing purposes is a best estimate approach.

4. Available system transient analyses of ATWS events indicate that WWER-1000 reactors, like western PWRs, have inherent protection against ATWS, including the inherent features to shut themselves down if the nuclear feedback is sufficiently negative. However, except for the Temelin-specific design verification analyses for the diverse protection system, no complete and systematic ATWS analyses for WWER-1000 plants have yet been presented for rigorous review by the regulatory authorities.

5. The various control and limitation functions of the WWER-1000 reactor also provide a degree of defence against ATWS. These functions are more numerous than on most western PWRs. Such functions generally enhance defence in depth by (a) reducing challenges to the reactor scram system and (b) by mitigating ATWS events. Some of these features can, however, introduce new event sequences requiring evaluation, e.g. MCP trip on low SG water level. (Further, reliability assessments are required to demonstrate that the same common mode failure will not affect other functions than reactor scram.)

6. It is not expected that any reasonable ATWS scenario for a WWER-1000 reactor could lead to pool boiling in the core and condensation of steam to boron-free water in the steam generators. A considerable reduction of the coolant inventory in the RCS would be required to disrupt single- or two-phase natural circulation completely. The situation appears to be more adverse on a WWER-440 with loop seals in the hot legs. This statement requires further verification.

7. Guidance on performing ATWS analyses of system transients for licensing purposes has been provided in Section 4. The relevant initiating events for WWER-1000 reactors are

identified and a best estimate approach to the transient analysis of ATWS events is recommended.

8. A reliability assessment of I&C related to ATWS events needs to be conducted, either prior to or in parallel with system transient analyses for ATWS events. This reliability study must use WWER-specific data for failure rates and operating experience. Attention should be given to determining that the same common mode failure cannot affect several of the required I&C functions.

9. Components and systems necessary to mitigate ATWS events need to be qualified for ATWS conditions. Examples of such conditions are water flow through pressurizer relief and safety valves and capability of ECCS valves to function after pressure peaks.

10. Provided that single- or two-phase natural circulation cannot be sustained due to reduction of the primary coolant inventory, special attention has to be given to the formation of diluted water slugs in the steam generators or at their outlets. Care is then required during recovery procedures to avoid recriticality in the core. The phenomenology of re-establishing natural circulation when the RCS inventory is restored requires further study. This issue is not unique to ATWS events or to WWER reactors.

11. Management of ATWS events has to be included in emergency operating procedures.

12. The development of a national policy on the ATWS issue in line with international practices needs to be established by national Regulatory Authorities. This policy should consider the systems necessary to mitigate consequences and/or requirements on acceptable plant performance in an accident with ATWS as the initiating event.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues and their Ranking for WWER-1000 Model 320 Nuclear Power Plants, IAEA-EBP-WWER-05, Vienna (1996).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Anticipated Transients without Scram for WWER-1000 Reactors, WWER-SC-186, 1996 (Report to the Steering Committee).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Accident Analysis of WWER NPPs, IAEA-EBP-WWER-01, Vienna (1995).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Evaluation, External Audit of NPP Dukovany, European Nuclear Assistance Consortium, WWER-440/213, Vienna ,1996.

[5] OPB-88, General Provisions for Enhancing the Safety of NPPs, PNAE-G-1-011-89, Moscow (1989).

[6] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, ASME Boiler and Pressure Vessel Code, Section III, NB-3234, ASME, New York (1995).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Rod Drop Issue for WWER-1000 Nuclear Power Plants, WWER-SC-214, 1998 (Report to the Steering Committee).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, General Design Safety Principles for Nuclear Power Plants, Safety Series No. 50-SG-D11, Vienna (1986).

ABBREVIATIONS

AMSAC	ATWS mitigation actuation system
ASME	American Society of Mechanical Engineers
ASSET	Assessment of Safety Significant Events Team (IAEA)
ATWS	anticipated transients without scram
AZ	emergency protection (Russian abbreviation), reactor scram
BDBA	beyond design basis accident
BNSA	Bulgarian Nuclear Safety Authority
BOC	beginning of cycle
BRU-A	steam dump valve to the atmosphere
BRU-K	stem dump valve to the turbine condensor
CMF	common mode failure
CR	control rod
DBA	design basis accident
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DPS	diverse protection system
ECCS	emergency core cooling system
ENAC	European Nuclear Assistance Consortium (Consortium of eight major western European nuclear design and engineering companies)
EOC	end of cycle
ESF	engineered safety features
FSAR	Final SAR
I&C	instrumentation and control
LOCA	loss of coolant accident
LOOP	loss off-site power
MCP	main coolant pump
MFP	main feed water pump
MTC	moderator temperature coefficient
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission (USA)
OECD	Organisation for Economic Co-operation and Development
PRP	primary reactor protection system
PSA	probabilistic safety analysis
PWR	pressurized water reactor
PZ	preliminary reactor protection (Russian abbreviation), preventive protection
RBMK	light water cooled, graphite moderated, channel type reactor (Soviet design)
RCS	reactor coolant system
ROM	power limitation controller (Russian abbreviation)
SAR	safety analysis report
SG	steam generator
TB	boron solution tank
TK	makeup system
TQn3	high pressure injection system
TQn4	high pressure boron injection system
URB	accelerated unit off-loading (Russian abbreviation)
WWER	water cooled, water moderated energy reactor (Soviet design)

CONTRIBUTORS TO DRAFTING AND REVIEW

Almeida, C.	International Atomic Energy Agency
Bassols, S.	Electricité de France, France
Benedetti, C.	International Atomic Energy Agency
Benisson, S.	Nuclear Regulatory Administration, Ukraine
Burnett, T.	Westinghouse Electric Corporation, United States of America
Fil, N.	OKB Gidropress, Russian Federation
Gerth, G.	Siemens, Germany
Hoehn, J.	International Atomic Energy Agency
Ivanova, A.	Energoproekt, Bulgaria
Langenbuch, S.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Germany
Lederman, L.	International Atomic Energy Agency
Lin, C.	International Atomic Energy Agency
Macek, J.	Nuclear Research Institute, Czech Republic
Malakhov, I.V.	Energoproekt, Ukraine
Misák, J.	International Atomic Energy Agency
Niehaus, F.	International Atomic Energy Agency
Philip, G.	International Atomic Energy Agency
Siltanen, P.	IVO International Ltd, Finland
Voznessenski, V.	RRC Kurchatov Institute, Russian Federation
Yoshimura, U.	International Atomic Energy Agency

Consultants Meeting

Vienna: 26–30 August 1996