SAFETY PHILOSOPHY OF THE OPERATING RBMK-1000 PLANTS

E.V. Burlakov (RRC KI), B.A. Gabaraev, Yu.M. Nikitin, A.A. Petrov, A.A. Potapov, (NIKIET),
N.M. Sorokin (Rosenergoatom)

ABSTRACT. The safety of the operating RBMK plants, the same as the safety of NPPs with other reactors, is based on the defence-in-depth philosophy. This philosophy has two strategic lines for safety enhancement. The one is accident prevention. The other is application of protective measures to mitigate the consequences of severe accidents and, if necessary, take additional measures to protect public and environment (emergency preparedness) even if such accidents have low probability. Accident prevention at the operating RBMK plants relies primarily on keeping all plant systems fully available all the time, in compliance with the "Maintenance Procedure for the RBMK-1000 Safety-Related Systems". A plant-specific high-priority document establishing rules and main requirements for the safe operation of the plant is "Technical Operation Rules". The inherent safety of RBMK reactors relies on the core configuration providing the following negative reactivity coefficients: temperature coefficients of fuel and of coolant, fast power coefficient. Besides negative reactivity effects, the inherent safety is associated with the fairly high level of natural circulation (~ 30 % N_{nom}) and slow progression of off-normal, transient and accident processes. At the same time, there is some deficiency in the inherent safety because of the positive feedbacks associated with positive reactivity coefficients, such as temperature coefficient of graphite (though graphite coefficient is of no importance in reactivity-induced accidents), void coefficient (which is currently maintained at the reactors in the range of 0.4÷0.8 β_{eff}) and voiding effect in the cooling circuit of the control and protection system (CPS) at full power.

As regards voiding of the CPS cooling circuit, this is a slow process. Moreover, reactivity variation due to the loss of water in the CPS circuit is much slower than the speed efficiency of the scram system. The safety analyses have shown that the safety systems provided at the operating RBMK plants ensure that the radiation consequences of the accidents caused by any initiating event considered in the design, will not exceed the dose limits specified in relevant regulations. Management of beyond-design-basis accidents may be provided using existing engineered features and emergency planning, i.e. additional organizational measures aimed at protection of personnel and the public.

To ensure fire safety, analysis was performed to investigate the impact of fires and their consequences on the safe shutdown and cooldown of the reactor system. Engineered and administrative measures were developed and implemented to protect the site and facilities against the natural and man-made events identified as a result of the analysis. A physical protection system was set in place. It is upgraded and renovated as dictated by the threats to the plant, nuclear materials and critical support systems. Due to the implementation of this philosophy, the risk associated with the operation of the RBMK plants meets the IAEA criteria established for the operating NPPs.

The design work on RBMK-1000 started in 1964. The first units with the capacity 1000 MWe – Leningrad 1 and 2 – were put in operation in 1973 and 1975, respectively. The safety of the first-generation RBMK plants was ensured proceeding from the requirements of special rules and regulations issued in the early 1970s, and general industrial requirements. The subsequent plants were built to the nuclear safety standards in force in the beginning of plant development. Today, the safety of the operating RBMK plants, which by 01.01.2007 had the operating record of more than 370 reactor·years, relies on the design-basis engineering solutions and on the upgrades and remedial measures implemented in the course of plant operation to bring the reactor safety as close as possible to the level demanded by existing regulations [1], [2], etc.

The safety assurance of the operating nuclear plants is based on the defence-in-depth philosophy which establishes several levels of defence to keep the potential radiological impact of the plant to a minimum achievable level in case of potential equipment failures and human errors, with adherence to the dose limits specified in relevant regulations [3] and [4]. Absolute priority is given to prevention and, if necessary, mitigation of off-normal events.

The principal instruments for avoiding parameter upset and preventing plant system / component failures (first level of defence) are site selection, quality assurance during design and performance of various activities, conservative approach to plant development with due regard for inherent safety mechanisms, and adherence to the safety culture principles during plant operation.

The RBMK sites were chosen so as to ensure safe operation of the plants taking into account possible natural phenomena, and external events in the selected areas. At present, the buffer area radius is set in the range from 1 km to 1.7 km. The controlled area radius ranges from 17 km to 19 km.

The quality of the implemented nuclear projects was provided relying primarily on the experience of production and power reactors designed, constructed and operated in the 1950s and 1960s, reinforced by a conservative approach.

System reliability at the operating RBMK plants is provided based on the Maintenance Procedure for the Safety-Related Systems at the RBMK-1000 Plants. System / component availability is checked as required by the Inspection and Testing Procedure for Safety-Related Systems, which specifies the scope and frequency of system inspections and tests and describes the terms under which the system may be removed from operation for inspection or testing. There is a special procedure for an in-service inspection of pressure tubes and graphite.

Of particular importance for the safe operation of the plants is the in-service inspection of pipelines and components in the reactor circulation circuit (RCC) and early detection of small leakages. The inspection scope and frequency are chosen so as to lower the probability of an instantaneous guillotine rupture of a large-diameter pipeline to less than 10^{-6} 1/reactor · year. Owing to a data bank on the detected defects, it is possible to perform selective checks and make trustworthy predictions concerning the state of components and pipelines in the periods between the inspections.

The key document at the plant level establishing rules and main requirements for the safe operation of the plant is Technical Operation Rules. Also, the plants have specific procedures describing operation of individual systems and components during startup, on-load operation, shutdown and outage.

Duties and rights of the personnel, staff interfaces and subordination, the list of equipment under custody, and the knowledge required of the staff – from plant shift supervisor to operator, are described in relevant job regulations. The skills required of personnel in normal and off-normal conditions are provided through studying relevant technical documents and regulations, operator training and examination on simulators. The operating record of the plants is periodically reviewed by the utility and in the framework of the ASSET missions, WANO peer reviews, IAEA and TACIS international projects. This takes care of the safety culture issues which call for a proper training and psychological preparedness of all people and organizations committed to safety assurance as a first priority.

The inherent safety features of the RBMK reactors which help avoid upsets in plant operation, are provided by core configuration which ensures the following negative reactivity coefficients: temperature coefficient of fuel $\alpha_t \sim -2.7\cdot10^{-3}\ \beta_{eff}$ /°C, fast power coefficient $\alpha_w \sim -2.3\cdot10^{-4}\ \beta_{eff}$ / MW, temperature coefficient of coolant $\alpha_{t\ H_2O} \sim -(1\div2)\cdot10^{-5}$ 1/°C. Also worth mentioning is very small reactivity margin for burnup compensation, possible due to the on-load refueling.

Besides the reactivity effects, the inherent safety of the reactor is associated with fairly intense natural circulation (~ 30 % N_{nom}) and slow progression of off-normal, transient and accident processes. This is provided due to:

- high heat capacity (~ $2.7\cdot10^6$ kJ/°C) and relatively high heat conductivity of graphite moderator;
- large water inventory in the reactor circulation circuit (~ 750 t);
- large steam inventory in the drum separator and in steam lines (~ 800 m^3), which prevents quick pressure variations in the reactor circulation circuit;
- long rundown time of the main circulation pumps (~ 2 min).

As follows from the analyses, there is no additional activity release from fuel rods in the initial stage of all loss-of-coolant accidents.

In incidents, the inherent safety features of the reactor – large dryout margin and small average linear power of fuel (q_1 ~ 150 W/cm) – help ensure normal heat removal from fuel claddings and provide sufficient time for plant parameter recovery.

At the same time, there is certain inherent safety deficiency because of the positive feedbacks associated with the positive reactivity coefficients, such as

- temperature coefficient of graphite $\alpha_c \sim (6\div7)\cdot10^{-3}\ \beta_{eff}$ / °C, though the heating of the graphite stack is a slow process due to the high heat capacity of graphite (time constant ~ 40 min.), so that this coefficient is of no importance in the reactivity-induced accidents;
- void coefficient, which is currently maintained in the reactors in the range of $\alpha_\varphi \sim$ 0.4-0.8 β_{eff}; the core voiding effect is close to zero or is negative; and
- voiding effect in the cooling circuit of the control and protection system (CPS) at full power $\rho_{CPS\ CC} \sim 1.5\div2\ \beta_{eff}$ (this effect is negative when the CPS rods are inserted in the core).

As regards voiding of the CPS cooling circuit, this is a slow process, and reactivity variation due to the loss of water in this circuit is much slower than the speed efficiency of the scram system. Further reduction of the CPS voiding effect is provided due to the introduction of the cluster-type control rods. According to the analysis, $\rho_{CPS\ CC}$ can be reduced to ~ 1 β_{eff}.

It should be mentioned that the above inherent safety deficiencies caused by the positive coefficients of reactivity – first of all, α_φ – are not an exclusive feature of pressure-tube RBMK reactors. In fact, they result from the safety approach towards RBMK design in the late 1960s. Thus, the change in the uranium-graphite ratio at Kursk-5 by cutting off the graphite brick corners provided reduction of the void effect to $\alpha_\varphi \sim -0.6\ \beta_{eff}$ and other negative coefficients. The advanced designs of modular pressure-tube power reactors with capacity 860 MWe, 1000 MWe and 1500 MWe, furnished with the containment, have negative void and other coefficients of reactivity responsible for the inherent safety of the reactor.

Management of operational upsets is the second level of defence of the physical barriers which consists in detection of potential failures during plant operation and management of anticipated operational occurrences. The control and protection system ensures reactivity control if the reactivity growth does not exceed the prescribed rate of 0.07 β_{eff}/s, reactor period is no less than 20 s, and the shutdown margin is more than 2 % in the core with maximum reactivity. Together with I&C systems of normal operation, this system controls the process and ensures adherence to the safe operation limits.

At present, the RBMK-1000 plants have the following safe operation limits:
- reactivity margin in terms of effective manual control rods: less than 30 rods;
- thermal power over 3550 MWth;
- linear power in fuel rods over 490 W/cm;
- dryout margin less than 1;
- graphite temperature over 750 °C;
- pressure in steam drum separator more than 7.9 MPa;
- flow rate in CPS cooling circuit less than 800 m^3/h;
- flow rate in CPS channel with inserted rod less than 2 m^3/h;
- specific activity of ^{131}I in reactor circulation circuit at steady-state operation over $3.7 \cdot 10^{-5}$ Bq/kg ($1 \cdot 10^{-5}$ Ci/kg)

The safety requirements for the fuel handling operations are described in relevant operating procedures.

The management of the radioactive waste is controlled by the environmental services at the plants. An independent environmental audit of the RBMK plants was completed in 2004. As written in the Audit Statement, the plants are operated with adherence to the nature protection laws, rules and regulations. Owing to the engineering and administrative improvements, the collective doses of personnel exposure have been reduced approximately 2.4 times compared with 1996, and the actual release of the noble radioactive gases in atmosphere has been reduced ~3.2 times.

If safe operation limits are violated, the defence-in-depth strategy prescribes accident management (See Table 1).

Table 1. Accident management configuration

	Event		
	Design-basis accident	Beyond-design-basis accident	
Management goal	Stay within the design-basis limits	Prevent severe damage / melting of the core and keep activity in the containment	Mitigate severe damage / melting of the core
Management task	Prevention of accident progression		Accident mitigation
Systems employed	Safety systems Normal operation systems used as intended	All available systems used even beyond their design functions and capabilities	

Management of design-basis accidents is the third level of defence; management of beyond-design-basis events makes the fourth level of defence.

Clearly, efficient management of off-normal events depends primarily on safety system availability, as a back-up to the natural feedbacks. The operating RBMK plants are equipped with the following safety systems:
- control and protection system (CPS) or integrated monitoring, control and protection system (IMCPS) with two independent shutdown systems;
- emergency core cooling system (ECCS);
- system of protecting reactor circulation circuit against overpressure;
- reactor cavity venting system;
- emergency power supply system;
- ultimate heat sink system.

An engineering assessment was performed for all safety and safety-related systems, to ascertain that they will fulfill their design functions considering a single failure. The assessment of the RBMK safety system capabilities, based on the accident analysis findings, has shown that all parameters of protective barriers (fuel rods; pressure boundary, including pressure tubes; confinement system boundary) will stay within the safe limits, with a margin, in practically all credible initiating events. No single failure was found in any safety system that could prevent the system to fulfill its safety function.

Table 2 describes the acceptance criteria used in the safety analysis. Adherence to acceptance criteria guarantees, conservatively, that the physical barriers on the way of radioactivity release in the environment will remain integral.

Table 2. Acceptance criteria

Safety barrier	Parameter indicating barrier integrity
Fuel pellet	Maximum temperature 2800°C Enthalpy below 710 kJ/kg
Fuel cladding	Maximum temperature 700°C
RCC pipelines	Maximum pressure 10.1 MPa
Pressure tubes	Maximum wall temperature 650°C at pressure ~ 7 MPa
Reactor cavity	Maximum excess pressure 210 kPa
Accident localization systems	Specific to plant generation

If the value of the parameter under investigation goes beyond relevant acceptance criterion, the barrier state is analyzed using more detailed models and boundary conditions.

An integral assessment of an accident is made considering the radiological consequences of the event. The radiation safety standards [3] and [4] establish the following radiological limits for the public in the first 10 days after a design-basis accident: no more than 50 mGy (5 rem) for the whole body; and no more than 500 mGy (50 rem) for thyroid gland.

As follows from the safety analyses, the above limits are not reached in any design-basis event.

Thus, the existing safety systems at the operating RBMK plants guarantee that the radiological consequences will remain within the limits prescribed in relevant regulations.

Personnel actions in case of design-basis accidents are described in the event-based Procedure for Management of Design-Basis Accidents, Incidents and Anticipated Operational Occurrences. Today, Symptom-Based Procedures are being introduced NPPs.

Management of beyond-design-basis accidents incorporates actions intended to prevent DBA progression to a beyond-design-basis accident, and to manage and mitigate the BDBA stages of the accident (fourth level of defence). To fulfill these goals, all available systems are to be used at the plant, even beyond their design capabilities and functions. Operator actions in case of beyond-design-basis accidents are described in the BDBA Management Procedure. The management strategy has been developed proceeding from the analysis of the accident sequences that may lead to a severe damage of the core and to the loss of integrity of the barriers on the way of radioactive release in the environment. According to this Procedure, the key objective in case of a BDBA is to recover and maintain the principal safety functions, and, if necessary, mitigate the accident consequences.

Management of beyond-design-basis events is complemented by administrative measures aimed at protection of personnel and the public – emergency planning (fifth level of defence).

As prescribed by SP AS-03 [4], the findings of the consequence analysis for the initial stage of BDBA are used to define the emergency planning area (first of all, to provide shelter and distribute iodine) and identify the evacuation planning area.

Criteria for making urgent decisions early in a radiation accident are listed in Table 3.

Table 3. Decision making criteria for radiation accident

Protective measures	Averted dose in the first 10 days, mGy			
	Whole body		Thyroid, lungs, skin	
	Level A	Level B	Level A	Level B
Shelter	5	50	50	500
Preventive distribution of iodine:				
- adults	-	-	250	2500
- children	-	-	100	1000
Evacuation	50	500	500	5000

If the exposure averted by the protective measures does not exceed Level A, there is no need to take measures that will upset the usual course of people's life, business and social activities.

If the exposure avoided due to the protective measures exceeds Level A but does not reach Level B, the decision on taking protective measures is made based on the justification and optimization principles, taking into account the actual situation and local conditions.

If the exposure prevented by the protective measures reaches and exceeds Level B, appropriate protective measures should be implemented, even if they upset the usual course of people's life, business and social activities.

The personnel and population protection plan incorporates two interrelated self-sufficient documents: personnel emergency protection plan and population emergency protection plan. A decision on the need for and sufficiency of the measures prescribed by these documents is made on a case-by-case basis, by studying the accident data, performing quick assessment of potential radiological consequences of the emergency release, and looking at the actual measurement data in the contaminated area.

Emergency drills are periodically performed at each plant. In addition to the plant personnel, the Emergency Response Centre of the nuclear utility Rosenergoatom, emergency response centres of engineering support and other relevant organizations take part in the drills. Usually, observes from other countries participate in the exercise.

Fire protection at the operating plants was provided in compliance with fire safety regulations for nuclear plants, which were in force at the time of plant design and construction and which basically meet the current requirements. Nevertheless, after Chernobyl the safety level of all operating plants was reviewed and safety upgrades were suggested, in particular, in the area of fire protection. Normally, a list of non-compliances with the latest requirements is produced during the plant upgrading and life extension, and a schedule is developed for remedying the non-compliance or taking corrective measures.

To ensure the fire safety, analyses were performed for all RBMK plants to investigate the impact of fires and their consequences on the safe shutdown and cooldown of the reactor system. The findings of the analysis were used as an input for developing appropriate safety measures. In particular, the measures included replacement of flammable heat insulation on the turbine hall roof, replacement of flammable elastron, fire protection of metal structures, cables, air ducts, etc.

Protection of the RBMK plants against natural and man-made impacts was initially addressed in the stage of plant design, based on the regulations in force at that time. In 1995, a new regulation was issued on Consideration of External Natural and Man-Made Events at Nuclear and Radiation Facilities [5]. The regulation served as a basis for taking measures to protect the plants against possible external impacts, primarily, against potential sources of shock wave and fire in the radius of 30 km.

The principal protective measure against an aircraft crash is the requirement to set the air routes at a safe distance from the site.

Physical protection of nuclear facilities is a part of the national security system. The current philosophy of the physical protection of nuclear plants consists in process protection against unauthorized intervention. A physical protection system has been set in place at the plants. It is upgraded and renovated as dictated by the threats to the plant, nuclear materials and critical systems. Threat identification is State prerogative. Prevention of sabotage and terrorism is the responsibility of the operating organization.

Due to the implementation of this philosophy, the risk associated with the operation of the RBMK plants now meets the IAEA criteria set for the operating NPPs.

Nomenclature.

BDBA - beyond-design-basis accident
CPS - control and protection system
CPSCC - CPS cooling circuit
DBA - design-basis accident
ECSS - emergency core cooling system
IMCPS - integrated monitoring, control and protection system
RCC - reactor circulation circuit
α_c - temperature reactivity coefficient of graphite, $\beta_{eff}/^oC$
α_φ - void reactivity coefficient, β_{eff}
α_t - temperature reactivity coefficient of fuel, $\beta_{eff}/^oC$
α_w - fast power reactivity coefficient, β_{eff}/MW
$\alpha_{t_{H_2O}}$ - temperature reactivity coefficient of coolant, $1/^oC$.
N_{nom} - nominal reactor power
$\rho_{CPS\ CC}$ - reactivity effect of voiding CPS CC

References

1. FEDERAL NUCLEAR AND RADIATION SAFETY AUTHORITY OF RUSSIAN FEDERATION. General Rules for Nuclear Plants Safety Assurance. OPB-88/97, PNAE G-01-011-97. Moscow, 1997.
2. FEDERAL NUCLEAR AND RADIATION SAFETY AUTHORITY OF RUSSIAN FEDERATION. Nuclear Safety Rules for Nuclear Reactors. PBYa RU AS-89, PNAE G-01-024-90, Moscow, 1990.
3. Radiation Safety Standards. NRB-99, SP 2.6.1 758-99, Minzdrav (Ministry of Health), 1999.
4. FEDERAL NUCLEAR AND RADIATION SAFETY AUTHORITY OF RUSSIAN FEDERATION. Health Rules for Design and Operation of Nuclear Plants (SP AS 03), SP2.6.1. 24-03, Moscow, 2003.
5. FEDERAL NUCLEAR AND RADIATION SAFETY AUTHORITY OF RUSSIAN FEDERATION. Consideration of External Natural and Man-Made Events at Nuclear and Radiation Facilities. PN AE G-05-035-94. Moscow, 1995.