ARTICLES

SYSTEM OF CRITERIA FOR DETERMINING, GUARANTEING, AND INCREASING THE SAFETY OF POWER PLANTS

R. R. Ionaitis

Safety is now one of the most important concerns. The safety of technical plants, especially power plants, i.e., their capability of limiting harm to people and damage to the environment during normal operation and in the case of accidents is of greatest concern.

The basic principles of shielding and safety of nuclear power plants include government regulation, substantiation of the need for atomic energy, shielding of people and the environment, optimization of the shielding and safety, implementation of the shielding in depth, application of the correct technical criteria, and others.

Shielding and safety are based on the correct technology and control, qualified guarantees, trained personnel, comprehensive assessments, and lessons of experience and research.

The following are employed to determine the safety level:

deterministic substantiation, i.e., cause-effect proof that a plant functions reliably with a sufficient margin with respect to admissible limits taking into account the single-failure principle;

probabilistic analysis of safety with a determination of the probability and risk of an accident taking into account additional failures; and,

analysis of the satisfaction of international and national standards, rules, as well as regulatory agencies.

There are many new requirements and especially formulations of these requirements, and for this reason it is often difficult to determine the degree to which a plant does or does not satisfy one or another requirement or formulation. Moreover, the rules and norms are created by regulatory agencies and mainly for the control and operating personnel. They are not adequately directed toward the builders of power plants (investigators, designers, and others). An important condition for building a reliable and safe plant is that the plant must satisfy standard principles and criteria (during design, construction, operation, and so on). These include, first of all, redundancy, variety, independence (functional and physical), safety, identification [1], stacked shielding, diversity, safe failure and others [2], shielding in depth, dissimilarity, longevity, automatic execution, possibility of verification, and others [3]. These principles are generalized in [4] and have now been incorporated in the national standards and rules [5, 6].

Concepts for the most important safety system of a power plant — the system that shuts down the plant (suppression) — are being developed on the basis of general safety principles [7-12]. Improvements are still being made to the basic principles of shielding and safety [13, 14]. However, there is no single document systematically expounding the technical criteria of the reliability and safety, which are employed for determining, guaranteeing, and increasing the safety of power plants. Such an attempt is made in the present paper.

Proposition. Analysis of a plant (process) with respect to a system of reliability and safety criteria can be employed to produce a clear and concise representation of the safety of the plant (or the process implemented in the plant). The crux of the analysis is that the reliability and safety of any plant or process can be assessed, guaranteed, and increased by systematic and comprehensive application of the 26 reliability and safety criteria that will be examined below.

It is suggested that a systems analysis be made of power plant safety and of its safety systems to determine whether or not the system of technical reliability and safety criteria are satisfied.
The present system of criteria is regarded as a tool for rapid expert assessment of the safety of plants now being designed as well as operating or improved plants for purposes of analyzing and comparing them (with prototypes and variants) and to determine bottlenecks and means for eliminating them (before and for the purpose of presentation to safety agencies).

**BRIEF DESCRIPTION OF CRITERIA**

**Criterion 1. Self-Shielding.** First, the power plant and its safety systems are designed to be self-shielding, so that plant safety is mainly guaranteed on the basis of natural feedbacks and processes. For example, in RBMK type water–graphite reactors, reactivity effects arising from loss of water in the coolant loops (first and control loops) are decreased to values less than \(1\beta_{\text{eff}}^*\) by enriching the fuel, by installing additional absorbers and organization of the flow-through part of organs which affect the reactivity with maximum displacement of water from the coolant channels, and others.

**Criterion 2. Equipment.** A reactor plant is equipped with technical safety means, such as a system for control, monitoring, and shielding, an independent shutdown system (when necessary), system for emergency cooling of the core, accident containment, as well as neutralization of dangerous gases (hydrogen, and others).

**Criterion 3. Maintenance of Functions.** The safety systems guarantee control during normal operation, shutdown of the reactor during design accidents, redundancy of the shutdown function with off-design failure of the main shutdown system, feeding and/or holding back the coolant in the core, containment of the accident and limitation of the consequences of the accident, as well as shielding from inflammation and/or explosion of gases (radiolytic hydrogen and/or hydrogen from the steam-zirconium reaction during an accident).

**Criterion 4. Structural Division of the System.** Each safety system includes the following subsystems: executive (realizing the shielding action), controlling (controlling the power plant and forming the emergency signals), control-diagnostic (controlling the safety system), and supply (power, coolant, ventilation).

**Criterion 5. Consistency of Execution of the Functions.** The safety functions (shutdown, emergency cooling, hydrogen neutralization, accident containment, and so on) are constantly in place, when the plant is operating and when the plant is shut down.

**Criterion 6. Automatic Operation.** The safety systems are actuated automatically when the process parameter (neutron-physical, thermohydraulic, technical) reaches an emergency value. These systems can possess buttons (keys) for manual actuation by the operator, which are installed on the main and backup control panels and in the central room.

**Criterion 7. Ensuring Fast Operation.** The speed of operation of the safety systems is higher than that of any of the accident processes and/or combinations of such processes which are to be suppressed (by a given system) and which cause the established safety limits to be exceeded. The concept of speed of operation includes the delay time of the controlling and executing subsystems and their speed of execution. A safety system is triggered with a well-founded short delay from the moment that an accident setting is reached. This criterion is satisfied most fully and deeply in the most important safety system — the emergency reactor shutdown system.

**Criterion 8. Safe Failure. Fault-Safety.** A safe failure is a failure during which the plant remains in a safe state without the implementation of any measures. In other words, a failure (single, contingent) which does not lead to dangerous consequences is safe.

Safe-failure systems are safety systems whose failure can give rise only to a spurious (unanticipated) triggering and not to degradation of the implementation of the functions which they must perform. In other words, such safety systems tend to be triggered spuriously rather than fail.

**Criterion 9. Structural Redundancy.** Structural redundancy, i.e., redundancy relative to the required volume (minimum required and sufficient for performing the assigned functions), is employed for all safety functions and systems. For this, backup elements are introduced into each safety system, the channels which form the emergency signals are backed up, the shutdown systems are duplicated, and so on.

**Criterion 10. Temporal Redundancy.** Temporal redundancy is achieved by increasing the speed of operation of the system over an above the value required according to calculations.

\[*\text{Effective fraction of delayed neutrons.}\]