ICS 27.120.20
CCS F 83

NB

ENERGY INDUSTRY GUIDING TECHNICAL DOCUMENT OF THE PEOPLE'S REPUBLIC OF CHINA

NB/Z 20249-2013

Guidance for use of probabilistic safety assessment for classification of functions for instrumentation and control system important to safety in nuclear power plants

概率安全评价在核电厂安全重要仪表和控制功能分类中的应用指南

Issued on: June 8, 2013 **Implemented on: October 1, 2013**

Issued by: National Energy Administration of the PRC

Table of Contents

Foreword

This document was issued on 8 June 2013 by the National Energy Administration of the PRC and takes effect on 1 October 2013.

It is a NB/Z guiding technical document: it does not oblige, it guides.

It is classified under ICS 27.120.20, Chinese classification F 83.

This guiding technical document was drafted in accordance with the rules given in GB/T 1.1-2009.

This guiding technical document was prepared by the redrafting method with reference to IEC/TR 61838:2009 Nuclear power plants - Instrumentation and control systems important for safety - Use of probabilistic safety assessment for the classification of functions; the degree of correspondence with IEC/TR 61838:2009 is non-equivalent.

This guiding technical document was proposed by the Nuclear Power Standardization Technical Committee of the Energy Industry.

This guiding technical document is under the administration of the Nuclear Industry Standardization Research Institute.

Drafting organizations of this guiding technical document: CGN Engineering Co., Ltd.;

Shenzhen CGN Engineering Design Co., Ltd.

Main drafters of this guiding technical document: Sun Wei, Zhang Huanxin, Sun Yongbin, Guo Zhiwu, Yang Jie, Li Youran, Gu Pengfei, Zhang Longqiang, Jiang Hui, Liu Aiguo, Yang Chunju.

1 Scope

NB/Z 20249-2013 is the Chinese guiding technical document for using probabilistic safety assessment to classify the instrumentation and control functions important to safety in a nuclear power plant. It exists because the classification decides the cost and the schedule of everything downstream, and the traditional way of making it is blunt. Every I and C function is placed in category A, B or C, and that letter determines the qualification the equipment must pass, the redundancy and separation it must have, the software development rigour it must follow and the testing it must undergo; a function classified one letter too high is paid for many times over, one classified too low is a gap in the defence. The deterministic method in GB/T 15474 assigns the letter from the role the function plays in the design basis events, which is sound but takes no account of how likely those events actually are or of how much a given function really contributes to risk. This document adds the probabilistic view as a supplement, not a replacement: it uses the accident sequences, the core damage frequency and the importance measures of a Level 1 PSA to test and refine the deterministic classification, so that effort is concentrated where risk actually is. It defines the twenty-two terms the method needs, from accident sequence and event tree through common cause failure, screening and uncertainty to controlled state and safe shutdown; it sets the general principles, including the requirement that the deterministic and the probabilistic design be iterated against each other rather than used in isolation; it defines the three function categories and their relation to the safety systems and safety-related systems of HAD 102/14; and it gives the application method and the implementation steps. Three informative annexes cover the limitations of using either method alone, the way PSA classification is applied in other countries, and the application methods and results of PSA. The document was prepared with reference to IEC/TR 61838:2009. It was issued on 8 June 2013 by the National Energy Administration and took effect on 1 October 2013.

This guiding technical document gives the method, the general principles and the implementation steps for the classification of instrumentation and control (I and C) functions on the basis of risk-informed probabilistic safety assessment (PSA) techniques.

The classification method given in this guiding technical document applies to the classification of the functions of I and C systems important to safety in pressurised water reactor nuclear power plants; nuclear power plants of other reactor types may apply it by reference, according to their actual technical characteristics. Depending on the purpose, the methods concerned may be used in the design, construction, operation and

decommissioning phases of a nuclear power plant.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only the edition cited applies to this document. For undated references, the latest edition, including all amendments, applies to this document.

GB/T 12727 Quality qualification of electrical equipment of the safety system of nuclear power plants

GB/T 13630 Design of nuclear power plant control rooms

GB/T 15474-2010 Classification of instrumentation and control functions important to safety in nuclear power plants

GB/T 20438 Functional safety of electrical, electronic and programmable electronic safety-related systems

HAD 102/14 Instrumentation and control systems important to safety in nuclear power plants

IAEA NS-G-1.3:2002 Safety Guide: Instrumentation and control systems important to safety in nuclear power plants

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 accident sequence

A sequence of events leading to an undesired consequential state.

3.2 accident sequence analysis

The process of determining the combinations of initiating events, safety functions and system failures and availabilities that may lead to core damage.

3.3 anticipated operational occurrences (AOO)

The various operating processes deviating from normal operation that are expected to occur at least once during the operating lifetime of a nuclear power plant. Because appropriate measures have been taken in the design, such events do not cause serious damage to items important to safety and do not lead to accident conditions.

3.4 basic event

In a fault tree model, an event that does not need to be developed further because a suitable level of resolution has already been reached.

3.5 beyond design basis accident (BDBA)

Accident conditions whose severity exceeds that of the design basis accidents.

3.6 common cause failure

In a multi-channel system or in multiple systems, a failure in which one or more events cause two or more separated channels to fail simultaneously, so leading to the failure of the whole system or of several systems. A failure in which a specific single event or cause leads to the failure of two or more structures, systems or components.

3.7 core damage frequency

The expected number of core damage events per unit time.

3.8 design basis accident (DBA)

Those accident conditions against which a nuclear power plant has taken specific measures in the design according to established design criteria, and in which the damage to the fuel and the release of radioactive material remain within the regulatory limits.

3.9 design basis event (DBE)

A hypothetical event applied in the design in order to establish the acceptable performance requirements for structures, systems and equipment.

3.10 event tree

A logic diagram that starts from an initiating event or state and describes the progression of the accident through a series of branches representing the success or failure of the expected system or operator actions, finally reaching an end state of success or failure.

3.11 functions, and the associated systems and equipment (FSE)

The set of associated systems and equipment that carry out a given purpose or objective.

3.12 I and C function

The control, operation and/or monitoring carried out on a defined process.

3.13 I and C systems important to safety

Those I and C systems whose system failure or spurious operation could cause site personnel or the public to receive excessive radiation exposure, together with those I and C systems that prevent anticipated operational occurrences from leading to unacceptable consequences; they include the safety systems and the safety-related I and C systems.

3.14 initiating event

Any internal or external event that disturbs the steady operating state of the nuclear power plant and thereby gives rise to an abnormal event such as a transient or a loss of coolant