

ICS 27.120.20
CCS F 65

NB

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

NB/Z 20289-2014

**Guidelines for software verification and validation plan in
nuclear power plants**

核电厂软件验证和确认计划编制指南

Issued on: June 29, 2014

Implemented on: November 1, 2014

Issued by: National Energy Administration of the PRC

Table of Contents

Foreword	2
Introduction	3
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	1
3.1 Terms and definitions	1
3.2 Abbreviations	2
4 Software verification and validation	2
4.1 General	2
4.2 Software V and V planning	4
4.3 Detailed description of the V and V tasks	6
5 Guidelines for the SVVP	12
5.1 General	12
5.2 Purpose	12
5.3 Reference documents	13
5.4 Definitions	13
5.5 Overview of V and V	13
5.6 The V and V process	15
5.7 Reporting	29
5.8 V and V administrative procedures	30
5.9 V and V documentation requirements	35
Annex A (Informative) Software integrity levels and criticality analysis	36
Annex B (Informative) The eight topics of the SVVP	38
Bibliography	43

Foreword

This document was issued on 29 June 2014 by the National Energy Administration of the PRC and takes effect on 1 November 2014.

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 65.

This guiding technical document was drafted in accordance with the rules given in GB/T

1.1-2009.

This guiding technical document was prepared with reference to IEEE Std 1059-1993 Guide for Software Verification and Validation Plans and IEEE Std 1012-2004 Standard for Software Verification and Validation.

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: CNNC Control System Engineering Co., Ltd.; Beijing Guangli Nuclear System Engineering Co., Ltd.; State Nuclear Power Automation System Engineering Co., Ltd.

Main drafters of this guiding technical document: Ma Gang, Li Chaoli, Guo Xiaoxing, Wang Huaijing, Liu Rui, Tang Yi, Zhang Yadong, Li Lingpo.

Introduction

With the development of digital technology, software is increasingly widely applied in the instrumentation and control systems and in the electrical systems of nuclear power plants. By carrying out a series of software verification and validation (V and V) activities throughout the software life cycle it is possible to reveal software defects to the greatest possible extent and to guarantee the quality and the reliability of the software. Regulatory Guide 1.168 of the United States Nuclear Regulatory Commission endorses IEEE 1012, the second revision of RG 1.168 endorsing the 2004 edition of IEEE 1012. IEEE 1012 sets out the basic requirements for V and V and the content requirements for the software verification and validation plan (SVVP); IEEE 1059, as the companion standard to IEEE 1012, describes how to write an SVVP that meets the requirements of IEEE 1012.

This guiding technical document standardises and guides the writing of the SVVP. A properly written SVVP will effectively ensure that the V and V activities are carried out smoothly, and thereby guarantee the reliability of the software in the instrumentation and control systems and in the electrical systems of a nuclear power plant.

This guiding technical document is divided into five clauses. Clause 1 is the scope; Clause 2 lists the normative references; Clause 3 gives the terms, definitions and abbreviations used in this guiding technical document; Clause 4 gives the general principles of software V and V, the planning of software V and V, and a description of the main V and V activities that continue across the several phases of the life cycle, such as traceability analysis, evaluation, interface analysis and testing; Clause 5 discusses each part of the SVVP in turn and provides detailed guidance. In most cases the guidance for each part or task is presented in the form of a list of questions or activities. It should be noted that these lists

are not exhaustive, since other questions or activities will arise in any given situation; equally, not every item in a given list applies to every situation.

This guiding technical document also contains two annexes. Annex A describes and summarises the software integrity levels and the criticality analysis. Annex B gives the eight topics of the SVVP.

1 Scope

NB/Z 20289-2014 is the Chinese guiding technical document for writing the software verification and validation plan, the SVVP, for the instrumentation and control systems and the electrical systems of a nuclear power plant. It exists because digital technology moved the reactor protection system from relays into software, and software cannot be inspected the way a relay can. The defect that matters is the one nobody thought to look for, so the discipline is not to test at the end but to plan, from the first day of the project, exactly which evidence will be produced at each phase of the life cycle and by whom. That plan is the SVVP, and a project whose SVVP is vague produces V and V work that is vague. The document follows the international line the Chinese regulator recognises: it is built on IEEE 1012-2004, which sets the requirements for verification and validation and for the content of the plan, and on IEEE 1059-1993, which describes how such a plan is written; both are endorsed for nuclear use by Regulatory Guide 1.168 of the United States Nuclear Regulatory Commission. Clause 4 sets out the general principles - the nineteen quality attributes a project may specify, the requirement that each life cycle phase be verified against the phase before it, the requirement that the final product be validated against the established software and system requirements, and the requirement that the V and V effort be independent to a degree set by the criticality of the software. Clause 5 then walks through the SVVP section by section, from purpose and reference documents through the V and V process itself, reporting, administrative procedures and documentation requirements, giving for each part a checklist of the questions and activities to be considered. Two informative annexes cover the software integrity levels and criticality analysis, and the eight topics of the SVVP. It was issued on 29 June 2014 by the National Energy Administration and took effect on 1 November 2014.

This guiding technical document specifies the content of the software verification and validation plan (SVVP) for the instrumentation and control systems and the electrical systems of nuclear power plants, and provides specific guidance for the planning of the software verification and validation (V and V) work and for the preparation of the plan.

This guiding technical document applies to the writing of the SVVP for the instrumentation and control systems and the electrical systems of nuclear power plants.

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 9385-2008 Specification for computer software requirements specifications

GB/T 9386-2008 Specification for computer software test documentation

GB/T 11457-2006 Information technology - Software engineering terminology

NB/T 20063-2012 Instrumentation and control terminology for nuclear power plants

HAD 102/16 Computer-based systems important to safety in nuclear power plants

IEEE 1012-2004 IEEE Standard for Software Verification and Validation

3 Terms, definitions and abbreviations

3.1 Terms and definitions

The following terms and definitions apply to this document.

3.1.1 acceptance testing

a) Formal testing carried out to determine whether a system complies with its acceptance criteria and to enable the customer to decide whether to accept the system; b) formal testing by which the user, the customer or another authorised entity decides whether to accept a system or a component. [GJB 5234-2004, definition 3.1.1]

3.1.2 component testing

Testing carried out to verify the correct implementation of a software unit, or of a combination of related software units, and its conformity with the requirements of the programme.

3.1.3 life cycle model

A model that describes how the various activities of the software development process are performed. The life cycle model establishes the ordering constraints between the phases of software development and the criteria for each phase, and establishes the rules and constraints to be observed during the development process, so that the various activities and the personnel involved can be effectively coordinated and managed.

3.1.4 software verification and validation plan

A plan that describes how software verification and validation is to be carried out.

3.1.5 system testing

The activity of testing an integrated hardware and software system in order to verify and validate whether the system meets its original objectives. [GJB 5234-2004, definition