

ICS 27.120.99
CCS F 82

NB

**ENERGY INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

NB/T 20054-2011

Replacing EJ/T 1058-1998

**Nuclear power plants - Instrumentation and control system
important to safety - Software aspects for computer-based
system performing category A functions**

核电厂安全重要仪表和控制系统执行A类功能的计算机软件

Issued on: July 1, 2011

Implemented on: October 1, 2011

Issued by: National Energy Administration of the PRC

Table of Contents

Foreword	4
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	5
5 General requirements for the software project	5
5.1 Overview	5
5.2 Software types	7
5.3 Software development methods	8
5.4 Software project management	9
5.5 Software quality assurance plan	9
5.6 Configuration management	9
5.7 Software security	10
6 Software requirements	11
6.1 Software requirements specification	11
6.2 Self-supervision	12
6.3 Periodic testing	12
6.4 Documentation	12
7 Design and implementation	13
7.1 Principles of design and implementation	13
7.2 Languages and the supporting translators and tools	14
7.3 Specific recommendations	15
7.4 Documentation	16
8 Software verification	16
8.1 Software verification process	16
8.2 Software verification activities	17
9 Software aspects of system integration	19
9.1 General	19
9.2 Software related parts of the system integration plan	20
9.3 System integration	20
9.4 Verification of the integrated system	21
9.5 Defect resolution procedure	21

9.6 Software part of the integrated system verification report	21
10 Software aspects of system validation	21
10.1 General	21
10.2 Software aspects of the system validation plan	22
10.3 System validation	22
10.4 Software aspects of the system validation report	22
10.5 Defect resolution procedure	22
11 Software modification	22
11.1 General	23
11.2 Modification request process	23
11.3 Execution process of software modification	24
11.4 Software modification after delivery for use	24
12 Software aspects of installation and operation	25
12.1 Site installation of the software	25
12.2 Site software security	25
12.3 Adaptation of the software to the site environment	25
12.4 Training of operating personnel	25
13 Defence against software common cause failure	26
13.1 General	26
13.2 Software design for the prevention of CCF	27
13.3 Causes and effects of software induced CCF	27
13.4 Achievement of diversity	27
13.5 Balance of the advantages and drawbacks related to the use of diversity	28
14 Software tools for software development	28
14.1 General	28
14.2 Selection of tools	28
14.3 Requirements for tools	29
15 Quality qualification of pre-developed software	32
15.1 Overview	32
15.2 General requirements	32
15.3 Assessment and evaluation process	32
15.4 Requirements for the integration and modification of PDS in the system	36
Annex A (informative) Structural changes of this standard compared with IEC 60880:2006	39
Annex B (normative) Software safety life cycle and detailed software requirements	45

Annex C (normative) Detailed requirements and recommendations in the design and implementation process	47
Annex D (informative) Example of application-oriented software engineering	58
Annex E (informative) Languages, translators, link editors	61
Annex F (informative) Software verification and testing	64
Annex G (informative) Typical list of software documents	71
Annex H (informative) Matters to be considered for common cause failure and diversity ..	72
Annex I (informative) Tools for preparing and checking technical specifications, design and implementation	76
Annex J (informative) Requirements concerning pre-developed software (PDS)	78
Bibliography	80

Foreword

This document was issued on 1 July 2011 by the National Energy Administration of the PRC and takes effect on 1 October 2011.

It is a NB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

It is classified under ICS 27.120.99, Chinese classification F 82.

It replaces EJ/T 1058-1998, which is superseded.

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

This standard replaces EJ/T 1058-1998, Computer software for nuclear power plant safety systems, and EJ/T 1058.2-2005, Computer software for nuclear power plant safety systems, Part 2: Defence against software induced common cause failure, software tools and use of pre-developed software.

This standard is based mainly on EJ/T 1058-1998 and integrates part of the content of EJ/T 1058.2-2005. Compared with EJ/T 1058-1998 and EJ/T 1058.2-2005, apart from editorial modifications, the main technical changes are as follows.

The terms and definitions have been updated.

Symbols and abbreviations have been added.

Detailed content related to software V and V (verification and validation) has been added.

Requirements related to software common mode failure have been added.

Requirements related to software qualification have been added.

This standard is a modified adoption of IEC 60880:2006, Nuclear power plants,

instrumentation and control systems important to safety, software aspects for computer-based systems performing category A functions, using the redrafting method.

Compared with IEC 60880:2006, the structure of this standard has been considerably adjusted. Annex A gives a comparison table of the clause and subclause numbering of this standard and of IEC 60880:2006.

There are technical deviations between this standard and IEC 60880:2006. The main technical deviations are listed in the following paragraphs.

Common and easily understood terms and their definitions have been deleted, namely computer, computer program, data, initialization, safety function and software version.

In order to facilitate understanding, the terms robustness and security and their definitions have been added.

In order to suit the technical conditions of China, GB/T 16260 (all parts) is used in Clause 2, Normative references, in place of ISO/IEC 9126 (all parts). The degree of correspondence between the individual parts of the two standards is given in the following four paragraphs.

GB/T 16260.1-2006, Software engineering, Product quality, Part 1: Quality model (ISO/IEC 9126-1:2001, IDT).

GB/T 16260.2-2006, Software engineering, Product quality, Part 2: External metrics (ISO/IEC TR 9126-2:2003, IDT).

GB/T 16260.3-2006, Software engineering, Product quality, Part 3: Internal metrics (ISO/IEC TR 9126-3:2003, IDT).

GB/T 16260.4-2006, Software engineering, Product quality, Part 4: Quality in use metrics (ISO/IEC TR 9126-4:2004, IDT).

There are also editorial modifications between this standard and IEC 60880:2006. The main editorial modifications are listed in the following paragraphs.

The fifth paragraph and the sixth paragraph of Clause 1 have been deleted.

The first paragraph of 5.6 has been deleted.

The first paragraph of Clause 7 has been deleted.

The first paragraph of 7.2.1 has been deleted.

The first paragraph of Clause 12 has been deleted.

The first paragraph of 12.4.1 has been deleted.

The first paragraph of Clause 13 has been deleted.

The first paragraph of 14.1 has been deleted.