



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 28808-2021

**Railway applications - Communication, signaling and
processing systems - Software for railway control and
protection systems**

Issued on: December 31, 2021

Implemented on: July 1, 2022

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

foreword

Introduction

1 Scope

2 Normative references

foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents"

drafted:

This document replaces GB/T 28808-2012 "Rail traffic communication, signal and processing system control and protection system software", and

Compared with GB/T 28808-2012, in addition to structural adjustment and editorial changes, the main technical changes are as follows:

a) Deleted the following terms and definitions: 3:3 Usability, 3:5 Design Agency, 3:7 Elements, 3:11 Error Avoidance, 3:16 Product, 3:18 Reliable

3:19 Requirements Traceability Objectives (see Chapter 3 of the:2012 edition);

b) Added the following terms and definitions: 3:1:4 Component, 3:1:5 Configuration Administrator, 3:1:6 Client, 3:1:8 Entity, 3:1:16 Integration,

3:1:17 Integrator, 3:1:18 Existing software, 3:1:19 Open source software, 3:1:21 Project management, 3:1:22 Project manager, 3:1:23

Reliability, 3:1:24 Robustness, 3:1:25 Requirements Manager, 3:1:26 Requirements Management, 3:1:30 Security Functions, 3:1:33 Software Baselines,

3:1:34 Software Deployment, 3:1:41 Testers, 3:1:42 Testing, 3:1:43T1 Tools, 3:1:44T2 Tools, 3:1:45T3

class tools (see 3:1);

c) Changed the independence requirements of software management and organization (see Chapter 5, Chapter 5, Chapter 6, Chapter 7 of the:2012 edition);

d) Added requirements for software deployment and software maintenance (see 5:1);

e) the definition of roles involved in software development and the requirements for

individual competencies have been added (see 5:2);

f) new clauses on tools were added (see 6:7);

g) Added overall software testing and corresponding requirements (see 7:7);

h) Changed the requirements for software development outputs (see Appendix A, Appendix A of the:2012 edition);

i) Added Appendix C to further clarify the key capabilities of the software roles and their responsibilities (see Appendix C):

This document uses the redrafted law to modify and adopt IEC 62279:2015 "Control and Protection of Rail Transit Communication, Signaling and Processing Systems"

system software":

Compared with IEC 62279:2015, this document has made the following structural adjustments:

---3:1:9 corresponds to 3:1:10 of IEC 62279:2015;

---3:1:10 corresponds to 3:1:11 of IEC 62279:2015;

---3:1:11 corresponds to 3:1:9 of IEC 62279:2015;

---Appendix B corresponds to Appendix D of IEC 62279:2015, and adds the chapter number of each target and description;

---Appendix C corresponds to Appendix B of IEC 62279:2015;

---Appendix D corresponds to Appendix C of IEC 62279:2015:

The technical differences between this document and IEC 62279:2015 and their reasons are as follows:

--- Regarding normative reference documents, this document has made adjustments with technical differences to adapt to the technical conditions of our country and the circumstances of the adjustment:

The situation is reflected in Chapter 2 "Normative References", and the specific adjustments are as follows:

* Replace ISO 9000:2015 with GB/T 19000 which is equivalent to adopting international standards (see 6:5:4:2);

* Replace ISO 9001:2008 with GB/T 19001 which is equivalent to adopting international standards (see 5:1:2:1, 5:2:2:3, 6:4:1:2,

Table A:9 and Table C:11);

* Replace ISO /IEC 25010 (see 9:2:4:4, Table C:11) with GB/T 25000:10, which has been

modified to adopt international standards:

The following editorial changes have been made to this document:

- Deleted IEC 62278:2002 in the list of normative references in Chapter 2;
- Added description to indicate Appendix D (see 5:3:2:14);
- Added abbreviations "API" "CFG" "DSL" and "LCF";
- Changed references;
- Changed the error in IEC 62279:2015:
- * In 6:6:3, replace "(see 9:2:4:11)" with "(see 9:2:4:10)";
- * In Table A:1, the symbol "See Note 2" was originally marked in Documents No: 29, 30, and 31, and was changed to be marked in Documents No: 30, 31, and 32;
- * "Software Analysis Technology (6:3)" in Table A:8 is changed to "Software Analysis Technology (6:2)";
- * In Table A:9, "7:1" in the reference entry is changed to "6:5";
- * In Table A:12, the second serial number 9 and serial number 10 are changed to serial number 10 and serial number 11:

Please note that some content of this document may be patented: The issuing agency of this document assumes no responsibility for identifying patents:

Introduction

This document is used in conjunction with GB/T 21562 and GB/T 28809:

GB/T 21562-2008 is applicable to a wide range of rail transit systems, while GB/T 28809 is applicable to the entire rail transit control and prevention

Approval process for individual systems that may exist in the system: This document focuses on the use of software to provide software that meets safety integrity requirements:

method, the safety integrity is given to the software through a more comprehensive consideration:

This document provides a set of requirements for the development, deployment and maintenance of any safety-related components used in rail traffic control and protection applications:

All software should comply with these requirements: This document specifies relevant organizational structures, relationships between organizations, and development, deployment, and maintenance activities:

This document also provides guidelines for personnel qualifications and expertise:

The key concept of this document is the Software Safety Integrity Level (SIL): This document identifies five software safety integrity levels: SIL0~

SIL4, of which SIL0 is the lowest level and SIL4 is the highest level: The higher the risk of software failure, the higher the software safety integrity level:

higher:

This document clarifies the technologies and measures for five software safety integrity levels, and the technologies and measures required for SIL0~SIL4 are in Appendix A

listed in the normative table: The technical requirements required for SIL1 and SIL2 in this document are the same, and the technical requirements required for SIL3 and SIL4 are similar

same: This document does not give guidance on which software safety integrity level is appropriate for a given risk: because the decision

The policy depends on a number of factors, including the nature of the application, the extent of the security functions undertaken by other systems, and social and economic factors:

The process of assigning safety functions to software is defined by GB/T 21562 and GB/T 28809:

This document specifies the necessary measures to meet these requirements:

GB/T 21562 and GB/T 28809 require a systematic approach to:

- a) identify hazards, assess risks and make decisions based on risk criteria;
- b) determine the necessary risk reduction measures to meet the risk acceptance criteria;
- c) define a comprehensive system security requirements specification for the necessary security safeguards to achieve the required risk reduction;
- d) select an appropriate system architecture;
- e) the technical and managerial activities necessary for planning, monitoring and control that translate the safety requirements specification into

A safety-related system whose safety integrity is confirmed:

When decomposing the specification into a design consisting of safety-related systems and components, the safety integrity level needs to be further considered:

Step allocation, and finally form the required software safety integrity level:

At the current state of the art, whether it is the application of quality assurance measures