

ICS 25.040
CCS N 10



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

GB/T 21109.1-2022

Replacing GB/T 21109.1-2007

**Functional safety of safety instrumented systems in the
process industry sector - Part 1: Framework, definitions,
system, hardware and application programming requirements**

Issued on: October 12, 2022

Implemented on: May 1, 2023

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

Table of Contents

Preface	
Introduction	
1 Scope	1
2 Normative references	3
3 Terms and Definitions and Abbreviations	3
3.1 Terminology	3
3.2 Terms and Definitions	4
3.3 Abbreviations	19
4 Compliance with this document	21
5 Functional Safety Management	21
5.1 Purpose	21
5.2 Requirement	21
6 Safety life cycle requirements	24
6.1 Purpose	24
6.2 Requirements	26
6.3 Application SIS Security Lifecycle Requirements	27
7 verification	30
7.1 Purpose	30
7.2 Requirements	30
8 Process Hazards and Risk Assessment	31
8.1 Purpose	31
8.2 Requirements	31
9 Assigning security functions to protection layers	32
9.1 Purpose	32
9.2 Allocation process requirements	32
9.3 Requirements for the basic process control system as a protection layer	34
9.4 Requirements to prevent common cause, common mode and related failures	35
10 SIS Safety Requirements Specification (SRS)	35
10.1 Purpose	35
10.2 General requirements	35
10.3 SIS security requirements	35
11 SIS Design and Engineering	37

11.1 Purpose	37
11.2 General requirements	37
11.3 Requirements for system behavior when a fault is detected	38
11.4 Hardware Failure Margin	39
11.5 Requirements for equipment selection	40
11.6 Field devices	42
11.7 Interface	42
11.8 Maintenance or test design requirements	43
11.9 Quantification of random failures	44
12 SIS Application Development	45
12.1 Purpose	45
12.2 General requirements	45
12.3 Application programming	46
12.4 Implementation of the application	47
12.5 Application verification requirements (review and testing)	48
12.6 Requirements for application methods and tools	48
13 Factory Acceptance Test (FAT)	49
13.1 Purpose	49
13.2 Recommendation	49
14 SIS installation and commissioning	50
14.1 Purpose	50
14.2 Requirements	50
15 SIS Security Confirmation	51
15.1 Purpose	51
15.2 Requirements	51
16 SIS Operation and Maintenance	53
16.1 Purpose	53
16.2 Requirements	53
16.3 Inspection tests and inspections	55
17 SIS Modification	56
17.1 Purpose	56
17.2 Requirements	56
18 SIS Deactivation	57
18.1 Purpose	57
18.2 Requirements	57

19 Information and Documentation Requirements	57
19.1 Purpose	57
19.2 Requirements	57
Reference	59
Figure 1 Overall framework VII of GB/T	21109
Figure 2 Relationship between IEC 61508 and IEC 61511	2
Figure 3 Detailed relationship between IEC 61511 and IEC 61508	2
Figure 4 Relationship between safety instrumented functions and other functions	3
Figure 5 Programmable Electronic System (PES). Structure and Terminology	13

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 for Standardization Documents" drafting.

This document is part 1 of GB/T 21109 "Functional Safety of Safety Instrumented Systems in the Process Industry". GB/T 21109 has

The following parts were released.

--- Part 1. Framework, definition, system, hardware and application programming requirements;

--- Part 2. Application Guidelines for GB/T 21109.1;

--- Part 3. Guidelines for determining the required safety integrity level.

This document replaces GB/T 21109.1-2007 "Functional safety of safety instrumented systems in the process industry - Part 1. Framework, definition

Definition, system, hardware and software requirements", compared with GB/T 21109.1-2007, except for structural adjustment and editorial changes, the main technical changes

as follows.

--- Added the management requirements for personnel in functional safety management (see 5.2.2.3);

--- Added requirements for functional safety management system (see 5.2.5.2);

--- Increased the SIS designed and implemented according to the specifications, standards or practices before the publication of this document, and put forward requirements for users

(see 5.2.5.4);

--- Added new requirements for functional safety assessment, audit and revision (see 5.2.6);

--- Increased safety life cycle structure and planning requirements (see 6.2);

--- Increased application SIS security life cycle requirements (see 6.3);

--- Increased verification requirements (see 7.2);

--- Added requirements for SIS security risk assessment (see 8.2.4);

---Delete "additional requirements for safety integrity level 4", increase risk reduction requirements >10000 or average frequency of dangerous failures

Rate < 10-8/h inspection requirements and protection layer allocation requirements;

--- Added the requirements for the allocation of protection layers when the BPCS is not prepared to comply with this document (see 9.3.4);

--- Increased the relevant requirements of the application security requirements specification (see 10.3.3~10.3.6);

--- Added the safety manual requirements and SIF communication requirements in the SIS design and engineering requirements (see 11.2);

--- Increased the relevant requirements in the case of SIS bypass (see 16.2.3, 16.2.4, 16.2.7, 16.2.11);

--- Added the relevant requirements for SIS spare parts (see 16.2.12);

--- Increased review requirements for hazard and risk analysis, allocation and design of personnel responsible for performing operations and maintenance (see 16.2.13);

---Changed the behavior requirements of SIS in the case of power failure, expanded it to power source (including power supply, air, hydraulic source or pneumatic source)

SIS behavior requirements in case of failure (see 11.2.11, 11.2.11 of the.2007 edition);

--- Changed the system behavior requirements when a fault is detected (see 11.3, 11.3 of the.2007 edition);

--- Changed hardware failure margin requirements (see 11.4, 11.4 of the.2007 edition);

--- Changed the equipment selection requirements (see 11.5, 11.5 of the.2007 edition);

--- Changed the failure probability of SIF, changed it to the quantification of random failure and supplemented the relevant requirements of random failure quantification (see 11.9,

11.9 of the.2007 edition);