Chinastandards.org

ICS 25.040
CCS N 10

chinastandards.org - PREVIEW

# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

# GB/T 47698-2026

## Industrial internet - Specification for the safety integrity assessment of collaborative manufacturing platforms

工业互联网 协同制造平台安全完整性评估规范

**Issued on: May 25, 2026** **Implemented on: December 1, 2026**

**Issued by: State Administration for Market Regulation;**
**Standardization Administration of the PRC**

Preview: page 1 of 5 shown, 44 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-47698-2026

Chinastandards.org

# Table of Contents



chinastandards.org · PREVIEW

## 6 Safety Criticality Assessment Process

7.3.3 All software related to the execution of security functions shall undergo security criticality assessments and comply with the following requirements.

a) For C1 level software components, it should be confirmed that a failure will not negatively impact C2 or C3 level software components (this needs to be included). This includes analyzing the protective measures for these components, such as verifying, through checks on specified ranges, that data will not be written to C2 or C3 levels. (In components), when a negative impact is expected, it should be classified as level C2;

b) For C2-level components, it is necessary to verify that the implementation of their functionality will not lead to C3-level security-critical impacts (e.g., data integrity). The sex diagnostic function may cause data corruption during diagnosis, and there is no way to recover it.

c) For C3 level components, it is necessary to analyze and confirm whether C2 level components (monitoring, diagnostic, etc.) exist to ensure their security. A complete and critical downgrade.

7.3.4 The safety criticality assessment should at least include a deviation analysis and assessment of the module's operation in terms of timing, data, and state transitions, and



Preview: page 2 of 5 shown, 44 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-47698-2026

can be conducted using software. Methods such as HAZOP and FMEA were used to conduct keystone analysis. The parameters, lead words, meanings of lead words, and parameters were discussed. See Appendix A for examples of the meanings of conjunctions.

### 7.1 General Requirements

7.1.1 The expected functions to be performed by the collaborative manufacturing platform should be identified and clearly defined.

7.1.2 Based on the functions defined by the collaborative manufacturing platform, the platform should be divided into modules, and the specific unit modules included in each function should be clearly defined.

Note 1: A trade-off needs to be struck regarding the granularity of the functional module decomposition. If the granularity is too large, the coupling between security functions will be stronger, potentially leading to the corresponding modules only being able to... Achieve higher SIL targets. Note

2.The platform's internal functions, external interfaces, operating assumptions, and user manuals must be clearly described, and the collaborative manufacturing platform itself must be clearly listed. Specific items in the security integrity risk assessment include, for example, fault detection items in the platform's operating hardware environment, software self-test functions, and security input. Items such as security output items and cybersecurity threat items are described in documents such as architecture design and security requirements specifications.

7.1.3 The safety status, failure conditions, internal functions, external interfaces, operating assumptions, and usage conditions of all modules should be analyzed and determined. Items, etc.

7.1.4 Match all identified security functions of the collaborative manufacturing platform with the participating modules.

7.2 Safety Criticality Classification Criteria Each security function should be classified into security criticality levels for its respective functional module. Based on the mode of impact, security criticality can be categorized into... There are 3 levels, see Table 1.

### 7.3 Safety Criticality Classification Process and Methods

7.3.1 The safety criticality classification process is shown in Figure 5.

7.3.2 Safety criticality assessments should be conducted based on the hierarchical process shown in Figure

5.Hypothetical analysis assessment methods can be used, assuming deviations from the established criteria, and then analyzing the results. To assess whether it will lead to danger, the safety criticality assessment process is shown in Figure 6. Figure



Preview: page 3 of 5 shown, 44 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-47698-2026

### 7.4 Determination of Module Security Integrity Requirements

7.4.1 The SIL for each safety function should be determined according to Chapter 6, as well as the safety criticality of each module within the safety function, in accordance with the specifications in Table 2. Define the SIL requirements that each module should meet.

7.4.2 The premise for meeting the requirements of Table 2 is that different modules have sufficient independence. If the independence between two or more modules is difficult to achieve... If valid proof is obtained, then all associated modules should meet the highest SIL requirement.

7.4.3 In accordance with the requirements of GB/T 20438.1-2017, GB/T 20438.2-2017, and GB/T 20438.3-2017, determine the module's... Its security and integrity requirements include the security-related performance requirements of the module and execution time limits.

### 8.1 General Requirements

8.1.1 An evaluation should be conducted on all modules assigned SIL requirements to confirm that each module has correctly implemented its component safety functions. Yes, and it meets the corresponding safety and integrity requirements.

8.1.2 In accordance with the requirements of GB/T 20438.2-2017, the security-related modules of the collaborative manufacturing platform should be inspected from at least the following aspects. Security integrity capability assessment. hardware security integrity, system security integrity, behavior when a fault is detected, and secure data communication.

8.1.3 It should be assessed whether the platform has implemented sufficient information security protection measures, including.

a) Information security protection designs were developed based on typical industrial or sectoral requirements; Note

1.Such as the requirements of graded protection, and the requirements of industrial control information security standards such as GB/T 42456.

b) It should be analyzed whether the failure of different information security attacks may have a negative impact on security functions, and it should be determined whether all security functions have been adequately protected. Appropriate protection; Note

2.Consider using appropriate threat/vulnerability analysis methods.

c) It should be analyzed whether the designed information security protection measures themselves may have unacceptable negative impacts on the execution of security functions.

8.2 Hardware Security Integrity Assessment Conduct hardware security integrity



Preview: page 4 of 5 shown, 44 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-47698-2026

assessments in accordance with the requirements of sections

7.4.5 of GB/T 20438.2-2017.

Note. During the hardware security integrity assessment, it is necessary to consider that the collaborative manufacturing platform hardware may be a computer server, and the detection of its random failures is also important. Control may need to rely more on software.

### 8.3 Systemic Security Integrity Assessment

8.3.1 Conduct system security and integrity testing in accordance with the requirements of

7.4.7 of GB/T 20438.2-2017 and GB/T 20438.3-2017. Sexual assessment.

8.3.2 Based on compliance with 8.3.1, the following points should be emphasized in the design of collaborative manufacturing platform software.

a) Has the software code been tested and proven to comply with the relevant security coding standards? For any code that does not comply with the standards, sufficient [security measures should be taken]? Explain the rationale behind it.

b) In addition to the security function code, does the software itself have sufficient security mechanisms in place, such as defensive programming, code processing, etc. Program sequence monitoring, etc.; the ability of these security mechanisms to control software errors and random hardware failures should be analyzed and evaluated. Whether it is sufficient, for example, whether the corresponding diagnostic coverage has been achieved.

c) Design independence between different SIL modules or between security- and non-security-related modules; analysis of the impact of low-SIL modules on high-SIL modules. Do security-related modules, and non-security-related modules, have any unacceptable negative impacts on security-related modules?

8.3.3 Based on compliance with 8.3.1, the following points should be emphasized in the evaluation of collaborative manufacturing platform software verification.

a) Have software failure analyses been conducted on SIL2, SIL3, and SIL4 modules to demonstrate their effectiveness against reasonably foreseeable errors? Protective measures for each part;

b) Has the software code undergone sufficient testing, including static and dynamic testing? Does the dynamic testing meet the requirements? Test coverage as specified in GB/T 20438.3-2017;

c) Whether the tools involved in software development have undergone sufficient applicability verification.

8.4 Evaluation of behavior when a fault is detected

chinastandards.org · PREVIEW



Preview: page 5 of 5 shown, 44 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-47698-2026