ICS 25.040
CCS N 10

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47683-2026

Industrial internet - Specification for hazard analysis and risk assessment

工业互联网 危险分析和风险评估规范

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

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

Table of Contents

1 Scope

GB/T 47683-2026 is the Chinese national standard covering hazard analysis for an industrial internet installation - where the connection of plant to network creates hazards that neither the plant nor the network had alone, and how those are identified, analysed and rated. First edition, in force from 1 December 2026, published with GB/T 47698-2026 on the safety integrity of collaborative manufacturing platforms. It was issued on 25 May 2026 and takes effect on 1 December 2026, as a first edition. The document is under the responsibility of the China Machinery Industry Federation. This page is published from the official record of the 2026 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

Note. The above is only an example of a possibility. Users of this document need to develop a classification that meets user and regulatory requirements based on the specific

implementation situation.

7.2.4 The consequences classification should include factors affecting the industrial internet, such as personal injury, economic loss, business continuity impact, and environmental impact. Impacts include asset and reputational damage. The severity of consequences must be graded based on national laws and regulations, national standards, industry standards, and company documents. Classification.

7.2.5 The risk matrix should combine the probability of an event occurring and the severity of its consequences.

5 General Rules

5.1 Scope of Analysis and Risk Assessment The scope of Industrial Internet hazard analysis and risk assessment is shown in Figure 1, and should cover the Industrial Internet edge layer, network layer, platform layer, and industrial core layers. The business application layer consists of four logical layers and various application combinations.

---The edge layer connects to different devices and systems through various communication methods, collects massive amounts of data, and utilizes edge computing devices to implement the underlying layer. Data is aggregated and processed, and integrated into the cloud platform.

Note. Typical examples of devices and systems accessing the edge layer include. manufacturing/production equipment, data acquisition equipment, industrial communication equipment, industrial control equipment, and industrial control systems. Control systems, human-computer interaction devices, etc.

---The network layer is the network infrastructure that supports the operation of industrial internet platforms. The platform layer provides general data analysis and management, industrial model development and management, and other services to support the industrial application layer in carrying out industrial... application.

---The industrial application layer provides industrial applications for different industries and scenarios.

5.2 Principles for Security Risk Analysis and Assessment at Each Level of the Industrial Internet Industrial control equipment and systems typically incorporate functional safety systems as risk mitigation measures. This is to address the information risks introduced by Industrial Internet technology. Information security threats necessitate the implementation of information security risk mitigation measures at all levels of the Industrial Internet to ensure the availability and integrity of facilities and systems at each level. And confidentiality. Functional safety and information security must be considered during the hazard analysis and risk assessment process at each layer of the Industrial Internet.

---The risk analysis and risk assessment of the edge layer comprehensively considers the

risk reduction capabilities of functional safety measures and information security measures, as well as information security measures. The impact of safety measures on functional safety measures;

---In hazard analysis and risk assessment at the network layer, platform layer, and industrial application layer, information security measures should be considered to reduce the occurrence of hazardous events. Potential preventative capabilities, and the reliability and availability of equipment at each level, which could lead to hazardous events; the impact of hazardous events. When impacting field devices and control systems connected to the edge layer, attention should be paid to the ability of functional safety and other measures to mitigate the severity of the consequences.

6 General Requirements

6.1 Timing of Assessment Hazard analysis and risk assessment should be conducted at the following points.

---At least one hazard analysis and risk assessment should be conducted during the design phase.

---During the operational phase, hazard analysis and risk assessment should be conducted regularly. In the event of a major hazard incident in the same field, targeted hazard assessments should be implemented. Risk analysis and risk assessment. Note

1.The time interval is determined according to the specific circumstances, generally 3 to 5 years.

---A hazard analysis and risk assessment should be conducted after any major changes occur. Hazard analysis and risk assessment should be conducted during the disposal phase. Note

2.During the disposal phase, it is necessary to ensure that sensitive data is completely eliminated and that the risks of other related devices still in use are controllable.

6.2 Personnel Requirements

6.2.1 Members of the hazard analysis and risk assessment working group should be independent (as opposed to project design and operation), either from the project design personnel or the project team. Other relevant personnel in the group should cooperate with the analysis team in hazard analysis and risk assessment activities.

6.2.2 The working group members should include personnel with relevant experience in the Industrial Internet and knowledge of relevant laws and regulations to ensure the effectiveness of hazard analysis and risk assessment. The reasonableness and credibility of the risk assessment results.

6.2.3 The working group shall include personnel who have participated in functional safety and information security technology training and have the corresponding knowledge and experience.

Note. Regarding functional safety, personnel need to understand GB/T 20438 (all parts) [process industries also need to understand GB/T 21109 (all parts)] and obtain industry certification. Authoritative functional safety certification; in terms of information security, personnel need to understand GB/T 20986, GB/T 35673, and other standards for information security and industrial control system information security. Comply with relevant standards and obtain training certificates.

6.2.4 The working group should include at least one person with a relevant professional background in the industrial system to be evaluated (such as industrial control equipment, process flow, etc.). The term of service shall not be less than 3 years.

6.3 Management Requirements

6.3.1 The organization responsible for hazard analysis and risk assessment shall establish a hazard analysis and risk assessment working group and clearly define the responsibilities and independence of each member. Require.

Note. The organizers include the designers, builders, and users of the industrial system.

6.3.2 Personnel performing hazard analysis and risk assessment shall meet the requirements of 6.2.

6.3.3 The working group shall prepare a hazard analysis and risk assessment plan, which shall include the following contents.

---The objects and scope of hazard analysis and risk assessment.

Note. The scope of the assessment object, applicable laws, regulations, and standards must be clearly defined in the plan. The definition of the scope of work may also be related to the input data (such as design specifications). The level of detail (as in books, device drawings, etc.) is related to this.

---Activities required to be performed at each stage of hazard analysis and risk assessment.

---Personnel, departments, organizations, or other entities involved in hazard analysis and risk assessment activities.

---Resources needed to complete hazard analysis and risk assessment activities.

---Proposed tools and record sheets.

---The outputs that should be obtained after completing hazard analysis and risk assessment activities.