ICS 35.240.01
CCS L67

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44062-2024

Automation systems and integration - Safety evaluation for automated devices

自动化系统与集成 自动化设备安全评估

Issued on: May 28, 2024 **Implemented on: December 1, 2024**

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

Table of Contents

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: Please note that some of the contents of this document may involve patents: The issuing organization of this document does not assume the responsibility for identifying patents: This document was proposed by the China Machinery Industry Federation: This document is under the jurisdiction of the National Technical Committee for Standardization of Automation Systems and Integration (SAC/TC159): This document was drafted by: Beijing Institute of Automation of the Mechanical Industry Co:, Ltd:, Qingdao Institute of Standardization, and Youli Standards Technology Services (Shanghai) Co:, Ltd: Beijing Branch, Ninebot (Beijing) Technology Co:, Ltd: The main drafters of this document are: Guo Dong, Zhai Yue, Chang Ping, Jiang Jiang, Gao Yaping, Zhang Siguang, Yang Shuping, Si Jiashun, Yuan Wangtan, and Sun Xun:

To ensure that the safety of automation equipment is fully and continuously considered in an acceptable manner during the design process and throughout the system life cycle, The document provides evidence for safety automation equipment and proposes evaluation criteria that can be used to determine the acceptability of safety files: The safety files issued when guiding manufacturers, integrators, and component suppliers to design, manufacture, and evaluate automation equipment can prove the safety of automation equipment: The safety of equipment: This document uses mandatory elements, required elements, strongly recommended elements, recommended elements and compliance as normative elements to regulate safety The summary of the safety profile deviation methods for different types of elements is shown in Table 1: Table

1 Safety profile deviation method Summary of normative elements Mandatory elements do not allow for safety profile deviations Essential Elements Security profile deviations are only applied to requirements that are inherently inapplicable due to the fundamental nature of the project and/or the current deployment status of the project: All safety use case

deviations documented in the safety profile are justified: Tracking, monitoring the possibility of changes in suitability status Highly recommended elements Deviations from the safety profile are permitted when there are acceptable reasons: Monitoring through impact analysis and life cycle tracking Possibility of change in suitability status: All safety dossier deviations recorded in the safety dossier are justified Recommended elements are optional: They do not need to be mentioned in the safety dossier: Safety dossier deviations do not require supporting arguments: Compliance is assessed through self-audits and independent assessments to ensure compliance with each clause Automation system and integrated automation equipment safety assessment

1 Scope

GB/T 44062-2024 sets the Chinese approach to evaluating the safety of automated devices. As automation moves from fenced cells to machines that share space with people, the classical approach of guarding and interlocks is no longer sufficient on its own, and what a purchaser or an authority needs is a structured demonstration that the residual risk has been assessed and controlled. The standard is built around that demonstration. It sets the requirements on the safety file and the safety case, its style, form and content, then the evaluation process: the definition of the device, its intended use and its foreseeable misuse, the hazard identification, the risk estimation and evaluation, the assessment of the risk reduction measures including the performance level or safety integrity level of the safety functions, the verification and validation evidence required, the competence and independence of the evaluator, and the conclusion and the report. It takes effect on 1 December 2024.

This document specifies the compliance requirements for establishing and evaluating safety demonstration of automation equipment, mainly including safety files, risk assessment, etc: content: This document is intended to guide manufacturers, integrators, and component suppliers in the design, manufacture, and evaluation of automation equipment:

2 Normative references

This document has no normative references:

3 Terms and definitions

The following terms and definitions apply to this document: 3:1 acceptable Sufficient to achieve the overall project risk identified in the safety profile: Example: "Acceptable test coverage" means the amount of test coverage is sufficient to support the safety dossier for the overall project after the claimed risk reduction confidence is achieved: Statement of risk: NOTE: This is an objective term relating to the effectiveness and completeness of a safety profile, rather than a subjective term relating to the personal opinion of any particular assessor: the term: 3:

2 Inputs or conditions that cause a system to fail due to faults or hazards: Example: A corrupted bit in memory that is disturbed by a single event is considered a fault: When reading the memory location, the fault is triggered and causes a calculation error that can be expressed as an error: Correct or unsafe project behavior causes system failure: NOTE: Fault mitigation measures (e:g:, error detection coding) can prevent the triggered fault from causing a failure: 3:

3 Computational algorithms and other related techniques (including inductive learning, intentional non-deterministic behavior, rule-based systems, computer vision, general description of search and other techniques): NOTE: This term is a descriptive term that is interpreted broadly to cover software that is not generally amenable to traditional software security approaches: and "intelligent" aspects are outside the scope of this document: 3:4 argue process of constructing a safety profile (3:32) that meets specified requirements Example: "The developer shall demonstrate that all hazards have been reduced" means that the developer shall include in the safety dossier a statement and evidence that each hazard has actually been reduced: and evidence: 3:5 assessor The person or persons who carry out the assessment: