

ICS 25.040
CCS N 10



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

GB/T 44861-2024

**Security for industrial automation and control systems -
Security risk assessment for system design**

工业自动化和控制系统安全 系统设计的安全风险评估

(English Translation)

Issued on: October 26, 2024

Implemented on: May 1, 2025

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

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms, Definitions, Abbreviations and Conventions
4 Area, Pipeline and Risk Assessment Requirements
4.1 Overview
4.2 ZCR1.Recognition of SUC
4.3 ZCR2.Initial Cybersecurity Risk Assessment
4.4 ZCR3.Dividing SUC into regions and pipelines
4.5 ZCR4.Risk Comparison
4.6 ZCR5.Perform a detailed cybersecurity risk assessment
4.7 ZCR6.Document cybersecurity requirements, assumptions, and constraints
4.8 ZCR7.Asset Owner Approval
Appendix A (Informative) Safety Level
Appendix B (Informative) Risk Matrix
Reference

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 equivalent to IEC 62443-3-2:2020 "Industrial automation and control systems safety - Part 3-2.Safety of system design" risk assessment".

The following minimal editorial changes have been made to this document.

--- To coordinate with the existing standards, the name of the standard will be changed to "Safety Risks in System Design for Industrial Automation and Control Systems" Evaluate".

Introduction

There is no easy way to ensure the security of Industrial Automation and Control Systems (IACS) because security is a risk management Because of the threats faced, the likelihood

of these threats, the inherent vulnerabilities in the system, and the consequences of the system being damaged, Because IACS are different, they bring different risks to the organization. In addition, different organizations have different tolerance for risks.

This document is intended to guide organizations in assessing the risks of specific IACS and identifying and applying safety countermeasures to reduce the risks to an acceptable level.

The key concepts in this document are the application of areas and pipelines, as defined in GB/T 40211.

Users of this document include asset owners, system integrators, product suppliers, service providers and compliance management agencies.

This document provides a framework for determining security countermeasures by agreeing on the Security Level of Target (SL-T) and the Security Level of Capability (SL-C). in accordance with.

Industrial Automation and Control System Security Security risk assessment of system design

1 Scope

This document specifies requirements for.

- a) Determine the System Under Assessment (SUC) of the Industrial Automation and Control System (IACS);
- b) Delineate the areas and pipelines of SUC;
- c) assess the risk of each area and pipeline;
- d) Establish target safety levels (SL-T) for each area and pipeline;
- e) Document safety requirements.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

GB/T 35673-2017 Industrial Communication Networks Network and System Security System Security Requirements and Security Levels (IEC 62443-3-3:2013,IDT)

3.1 Terms and Definitions

The following terms and definitions apply to this document.

The URLs for terminology databases used for standardization maintained by ISO and IEC are as follows.

3.1.1

channel

A specific logical or physical communication link between assets.

NOTE: Channels help establish connections.

3.1.2

Compliance Authority the entity with the authority to determine the adequacy or effectiveness of the implementation of a safety assessment specified in the governing documents.

NOTE Examples of compliance management bodies include government agencies, regulatory bodies, and external and internal auditors.

3.1.3

conduit

A logical grouping of communication channels connecting two or more areas with the same security requirements.