



中华人民共和国国家标准

GB/T 46933.2—2025

智能工厂安全一体化 第2部分：风险评估要求

Safety and security integration of smart factory—
Part 2: Risk assessment requirements

2025-12-31 发布

2026-07-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 一般要求 3

 5.1 评估对象 3

 5.2 评估要求 3

6 风险评估准备活动 3

 6.1 确定安全目标和风险可容忍准则 3

 6.2 确定风险评估范围 4

 6.3 组建评估管理与实施工作组 4

 6.4 评估资料准备 4

 6.5 选择评估工具和方法 5

 6.6 制定风险评估计划 5

7 风险评估程序 5

 7.1 风险评估流程 5

 7.2 节点划分 6

 7.3 偏差确定 7

 7.4 危险识别 7

 7.5 威胁和脆弱性识别 8

 7.6 危险事件分析 9

 7.7 危险事件发生可能性分级 10

 7.8 后果分析 10

 7.9 后果严重程度分级 10

 7.10 初始风险评估 11

 7.11 风险降低措施分析 11

 7.12 保护/防护能力评估 11

 7.13 残余风险评估 11

 7.14 意见建议 11

8 风险评估文档记录 12

附录 A(资料性) 风险评估方法 13

附录 B(资料性) 威胁示例 15

附录 C(资料性) 危险事件发生可能性评估示例 16

附录 D(资料性) 后果严重程度分级示例 19

附录 E(资料性) 风险矩阵示例 20

参考文献 21

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 46933《智能工厂安全一体化》的第2部分。GB/T 46933 已经发布了以下部分：

- 第1部分：一般要求；
- 第2部分：风险评估要求；
- 第3部分：系统协同设计要求；
- 第4部分：系统评测要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、中国石油集团安全环保技术研究院有限公司、国家石油天然气管网集团有限公司油气调控中心、中控技术股份有限公司、上海能源建设工程设计研究院有限公司、上海辰竹仪表有限公司、航天智控(北京)监测技术有限公司、上海液化天然气有限责任公司、宁波和利时信息安全研究院有限公司、中国石化青岛炼化有限责任公司、西电宝鸡电气有限公司。

本文件主要起草人：郭苗、刘瑶、魏振强、孙铁良、范咏峰、张晋宾、马欣欣、熊文泽、张鑫、梅恪、洪鹏达、侯明艳、张锋、张凯、吴海峰、张志强、张兆云、朱杰、孙永康、陈小全、曾志生、罗方伟、曹欣宜、周力、聂中文、帅冰、施隋靖、朱明露、任志刚、朱旭营、王振宇、李冠辉、刘盈、陈鑫、高龙波、杨柳、朱弘毅、刘万里。

引 言

传统工厂一般采用 GB/T 20438(所有部分)《电气/电子/可编程电子安全相关系统的功能安全》和应用领域标准(如 GB/T 21109(所有部分)《过程工业领域安全仪表系统的功能安全》、GB/T 16855(所有部分)《机械安全 控制系统安全相关部件》、GB 28526《机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全》)来实现功能安全,采用 GB/T 35673《工业通信网络 网络和系统安全 系统安全要求和安全等级》等标准来实现工控信息安全。在技术上,一般使用相对独立的电气电子可编程电子或机械保护系统,不同系统间一般是隔离的或有限的连接,功能安全系统和信息安全防护之间也相对独立设置。

随着智能工厂的发展,越来越多的智能化技术、信息技术被应用到工业控制系统中,智能工厂的各层级内和层级间的设备/系统实现了更为深入的互联互通。这提高了工业经营者的效率,降低了成本,却也增加了系统复杂程度,在传统生产运行风险控制方面带来新挑战。一方面,传统的功能安全技术措施(如安全仪表系统)面临更复杂的应用环境(如黑客攻击、恶意软件等信息安全威胁,人工智能 AI 的失控危险等),其原本的风险降低能力减弱;另一方面,外部影响因素增多、各单元相关性增强,使得原有的风险防护理论的适用性降低;最后,不同安全防护措施之间交互融合,彼此之间潜在的冲突和矛盾激增。因此,智能工厂需要采用安全一体化的方式来实现全生命周期的综合安全防护。

GB/T 46933《智能工厂安全一体化》旨在指导智能工厂建立安全一体化生命周期,并针对风险评估、系统协同设计和系统评测提出要求,拟由 4 个部分构成。

- 第 1 部分:一般要求。目的在于提出安全一体化生命周期的整体要求,以及实现安全一体化的基本原则。
- 第 2 部分:风险评估要求。目的在于提出开展安全一体化风险评估的流程和要求。
- 第 3 部分:系统协同设计要求。目的在于针对智能工厂制造执行层、过程监控层、现场控制层和现场设备层提出系统协同设计的要求。
- 第 4 部分:系统评测要求。目的在于提出开展安全一体化完善度评测的方法和要求。

本文件结合各领域智能工厂的架构模型以及自身特点,综合考虑智能工厂生产运行传统风险和由于互联互通、信息集成而带来的新风险,研究智能工厂生产系统风险评估对象、风险评估程序、风险评估相关活动、风险评估文档等内容和要求,凝练智能工厂安全一体化风险评估要素,提出智能工厂安全一体化风险评估的统一框架,建立起信息安全威胁和生产安全事件间的关联关系,目标是指导智能工厂将生产系统运行风险控制在可容忍范围之内。

智能工厂安全一体化

第2部分：风险评估要求

1 范围

本文件规定了智能工厂安全一体化风险评估一般要求、风险评估准备活动、风险评估程序、风险评估文档记录的要求。

本文件适用于对智能工厂生产系统开展安全一体化风险评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 46933.1—2025 智能工厂安全一体化 第1部分：一般要求

3 术语和定义

GB/T 46933.1—2025 界定的以及下列术语和定义适用于本文件。

3.1

伤害 harm

人身损伤、人的健康损害、财产或环境的损害。

[来源：GB/T 20438.4—2017, 3.1.1]

3.2

危险 hazard

伤害的潜在根源。

注：这个术语包括短时间对人身的伤害（如着火和爆炸），以及那些对人身健康长时间的损害（如有毒物质释放）。

[来源：GB/T 20438.4—2017, 3.1.2]

3.3

危险状况 hazardous situation

人、财产或环境暴露于一个或多个危险源环境的情况。

[来源：GB/T 20438.4—2017, 3.1.3]

3.4

危险事件 hazardous event

可能导致伤害的事件。

注：危险事件是否导致伤害取决于人、财产或环境是否遭受危险情况的后果，以及事件发生后，如果会对人产生伤害，人是否能避免该事件的后果。

[来源：GB/T 20438.4—2017, 3.1.4]