ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 46933.4—2025

智能工厂安全一体化
第4部分:系统评测要求

**Safety and security integration of smart factory—
Part 4:System evaluation 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

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4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、中控技术股份有限公司、陕西延长石油榆林可可盖煤业有限公司、国家石油天然气管网集团有限公司油气调控中心、上海能源建设工程设计研究有限公司、联通(陕西)产业互联网有限公司、东方电气集团数字科技有限公司、宁波和利时信息安全研究院有限公司。

本文件主要起草人：刘瑶、朱明露、刘全辉、帅冰、吕峰、梅恪、史学玲、朱杰、黄河、熊文泽、孙永康、吴海峰、武磊、郝鑫、任志刚、王晓鹏、刘立三、黄亮、李程鹏、范咏峰、杨柳、周有铮、赵艳领、马欣欣、周力、聂中文、张晋宾、裘坤、汪清仓、李守卿、刘盈、张亚彬、郭苗。

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、协同设计和评测验证提出要求,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。

本文件明确了智能工厂安全一体化评测的对象、目标、阶段、人员和活动要求,并给出了评测步骤、评测指标、评测方法,可指导相关各方对智能工厂功能安全和信息安全相互影响关系以及冲突消减/协同防护水平开展评测,以期实现智能工厂的高水平安全,为各生产领域的高质量发展提供安全保障。

智能工厂安全一体化
第4部分：系统评测要求

1 范围

本文件规定了安全一体化系统评测一般要求、系统评测实施要求以及系统评测报告要求。

本文件适用于用户、评测认证机构等独立或者非独立组织对智能工厂安全一体化协同程度进行相关的系统评测活动。

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 20438.4 电气/电子/可编程电子安全相关系统的功能安全 第4部分：定义和缩略语

GB/T 21109.1 过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和应用编程要求

GB/T 46933.1 智能工厂安全一体化 第1部分：一般要求

GB/T 46933.3—2025 智能工厂安全一体化 第3部分：系统协同设计要求

3 术语和定义

GB/T 46933.1、GB/T 20438.4、GB/T 21109.1界定的以及下列术语和定义适用于本文件。

3.1

风险降低因子 risk reduction factor；RRF

安全功能要求时危险失效概率（PFD）的倒数，是对安全功能所提供的风险降低能力的度量。

4 缩略语

下列缩略语适用于本文件。

DoS：拒绝服务（Denial of Service）

PHA：过程危险分析（Porcess Hazard Analysis）

P&ID：管道和仪表流程图（Piping and Instrumentation Diagram）

RRF：风险降低因子（Risk Reduction Factor）

SIF：安全仪表功能（Safety Instrumented Function）

SIL：安全完整性等级（Safety Integrity Level）

SL：信息安全等级（Security Level）

SSIL：安全一体化完善度（Safety and Security Integration Level）