ICS 13.100
CCS C 65

T/CS

团　　体　　标　　准

T/CS 426—2026

工业生产安全风险管控系统设计规范

Design specification for safety risk control system of industrial production

2026-06-24 发布　　2026-06-24 实施

中国商品学会　发布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总体设计要求 1
4.1 设计要求 1
4.2 责任主体 2
5 系统核心设计 2
5.1 风险辨识设计 2
5.2 风险评估设计 2
5.3 风险管控设计 4
5.4 风险预警设计 5
6 系统支撑设计 5
6.1 数据安全 5
6.2 运行维护 6

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。

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。

本文件由中国商品学会提出并归口。

本文件起草单位：宁波瑞航安全科技有限公司、宁波灵象电器有限公司、宁波恒雅机械有限公司、浙江时代京云标准科技有限公司、百家云（宁波）标准技术服务有限公司。

本文件主要起草人：聂亮、俞敏杰、杨海翔、怀志婷、吴彤。

工业生产安全风险管控系统设计规范

1 范围

本文件确立了工业生产安全风险管控系统的系统核心设计和系统支撑设计，并规定了风险辨识、风险评估、风险管控、风险预警等内容。

本文件适用于工业企业及相关方进行安全风险管控系统的规划、设计与开发。

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 13861 生产过程危险和有害因素分类与代码

GB/T 27921 风险管理风险评估技术

GB/T 33000 大中型企业安全生产标准化管理体系要求

GB/T 41260 数字化车间信息安全要求

GB/T 45001 职业健康安全管理体系 要求及使用指南

AQ 3035 危险化学品重大危险源安全监控通用技术规范

YD/T 4981 工业领域重要数据识别指南

YD/T 4982 工业企业数据安全防护要求

3 术语和定义

GB/T 33000界定的及以下术语和定义适用于本文件。

3.1

风险点 risk point

风险伴随的设施、部位、场所和区域，以及在设施、部位、场所和区城实施的伴随风险的作业活动，或以上两者的组合。风险点有时亦称为风险源。

[来源：GB/T 23694 风险管理 术语改写]

3.2

预警阈值 early-warning threshold

指风险预警中设定的监控参数临界值。当风险指标值达到或超过该值时，系统应发出预警信号。预警阈值与预警区间相对应，用于划分不同的预警等级。

[来源：GB/T 23694 风险管理 术语改写]

4 总体设计要求

4.1 设计要求

工业生产安全风险管控系统的设计，应遵循以下基本要求：

a) 系统性要求：构建覆盖工业生产、检修、停产等各阶段的风险防控体系；
b) 风险导向要求：系统设计应以风险辨识与评估为核心，将风险管控作为系统运行的基本出发点，系统应支持针对不同风险等级采取差异化管控措施；
c) 持续改进要求：系统应建立自我完善机制，根据评估结果、外部环境变化和绩效监测信息持续改进管理措施；
d) 闭环管理要求：系统应实现风险辨识、评估、控制、预警、响应、评审和改进等环节的信息联动。

4.2 责任主体

系统建设与运行管理的责任主体要求如下：

a) 企业主要负责人对本企业安全生产工作全面负责；
b) 其他负责人对职责范围内的安全生产工作负责；
c) 不同岗位人员参与风险辨识、评估、管控和预警等业务活动。

5 系统核心设计

5.1 风险辨识设计

5.1.1 风险辨识设计应符合下列要求：

a) 功能模块应支持对工业生产活动中各类风险点的辨识；
b) 功能的设计应符合GB/T 13861规定的危险和有害因素分类框架；
c) 风险辨识应覆盖人的因素、物的因素、环境因素和管理因素四个方面。

5.1.2 风险辨识相关数据的采集方法：

a) 人工录入数据：通过表单手动录入风险点信息；
b) 设备检测数据：通过接口采集传感器、监控设备等实时数据；
c) 外部系统数据：通过外部系统获取关联信息。

5.1.3 风险辨识与评估功能方法的选择和应用可参照GB/T 27921。

5.1.4 多层级风险辨识的组织协同要求如下：

a) 企业决策层、管理层、执行层在系统内分别开展不同层级和范围的风险辨识工作；
b) 上级对下级辨识结果进行审核、补充和汇总；
c) 多部门协同辨识，避免风险辨识的成果被遗漏或重复。

5.1.5 风险辨识结果的生成的风险点清单宜包含以下信息：

a) 风险点名称及编号；
b) 风险点所属位置（部门/车间/岗位）；
c) 风险点类型（设备设施/作业活动/场所区域）；
d) 危险有害因素分类（人的因素/物的因素/环境因素/管理因素）；
e) 可能导致的事故类型；
f) 现有控制措施。

5.2 风险评估设计

5.2.1 风险评估功能模块应支持对辨识出的风险点进行分析和评价，确定风险程度。

5.2.2 系统应支持风险值计算模型的配置，包括计算公式、参数取值范围及计算规则。

5.2.2.1 根据评估对象的特点和评估目的，选择适用的计算公式。常见的计算公式包括LS法（R = L × S）、LEC法（D = L × E × C）和MES法（R = M × E × S），各常见分类见表1。

表 1 常见分类

项目	内容
L（可能性）	事故或风险事件发生的可能性大小
S（严重性）	事故后果的严重程度
E（暴露频率）	人员暴露于危险环境的频繁程度
C（后果）	发生事故可能造成的后果
M（控制措施状态）	现有风险控制措施的有效性状态

5.2.2.2 计算规则的编排应包括以下内容：

a) 参数取值与分值的映射规则；
b) 多参数组合的计算顺序和权重设置；
c) 风险等级的划分规则；
d) 计算结果的精度控制和舍入规则。

5.2.3 系统应内置风险评估方法库，支持以下评估方法的选择和应用：

a) 风险矩阵分析法（LS）：适用于风险的半定量评价；
b) 作业条件危险性分析法（LEC）：适用于作业环境的危险性评价；
c) 风险程度分析法（MES）：适用于多因素综合风险评估。

5.2.4 企业可在以下风险判定准则的预设模板的基础上进行选取和调整：

a) 可能性（L）评分准则：预设发生频率、偏差发生率等评分维度和取值标准；
b) 后果严重性（S）评分准则：预设人身伤害、财产损失、环境影响等方面的严重程度分级；
c) 风险可接受准则：预设风险可接受阈值，区分可接受风险、需关注风险和不可接受风险,具体见表2；
d) 风险等级划分准则：预设风险等级划分标准及对应的管控要求。

表 2 风险等级

项目	内容
可接受风险	不会导致人员伤害或者财产损失小于一万元
需关注风险	会导致人员轻伤或者造成财产损失小于等于五十万元
不可接受风险	会造成人员重伤、死亡、多人伤亡或者造成财产损失大于五十万，甚至对环境、社会造成严重影响

5.2.5 风险评估报告内容宜包括以下信息：

a) 风险点基本信息（名称、编号、位置、类型）；
b) 采用的评估方法及评估准则；
c) 风险值计算过程和评估结论；
d) 风险等级或风险程度；

e） 风险排序；
f） 需要优先处理的风险及处理建议。

5.2.6 风险评估全过程的信息记录应包括以下内容：

a） 风险评估计划的编制和管理，包括确定风险评估目的和范围、理解评估背景、明确利益相关方的参与等；
b） 风险评估过程的在线记录，包括评估人员、评估时间、评估依据、评估结论等信息；
c） 风险评估结果的审核和确认流程；
d） 评估结果的版本控制。

5.3 风险管控设计

5.3.1 风险管控功能模块应支持对辨识和评估后的风险点实施有效管控。

5.3.2 建立维护风险点与管控措施之间的关联关系。一个风险点可关联多个管控措施，一个管控措施也可适用于多个风险点。

5.3.3 风险管控措施宜从工程技术措施、管理措施、培训教育、个体防护、应急处置等方面进行设计和实施。措施类型应按照GB/T 45001中规定的控制层级进行设计。系统应具备以下风险管控措施：

a） 消除危险源：完全消除危险源的措施；
b） 替代：当危险源无法完全消除时，应采用危险性较低的过程、操作、材料或设备进行替代；
c） 工程控制：采用工程技术手段降低风险，包括物理隔离、防护装置、机械防护等；
d） 管理控制：制定安全操作规程、完善管理制度、加强教育培训、建立作业许可制度、实施安全监督检查等管理手段控制风险；
e） 个体防护：在上述措施均无法将风险降至可接受水平时，应配备并使用适当的个体防护装备。

5.3.4 风险管控清单宜包含以下信息：

a） 风险点名称及编号；
b） 风险点所属位置（部门/车间/岗位）；
c） 风险点类型（设备设施/作业活动/场所区域）；
d） 风险描述；
e） 风险等级或风险程度；
f） 管控措施；
g） 责任部门；
h） 责任人；
i） 管控措施的实施状态及完成时限。

5.3.5 系统应支持风险管控措施的实施跟踪和效果验证功能，包括以下内容：

a） 管控措施的动态跟踪，系统应以任务分配的方式将每项管控措施落实到具体责任人，并设置完成时限和提醒机制；
b） 管控措施实施进度的在线填报和状态更新，记录实施过程中发现的问题和调整情况；
c） 管控措施实施后的效果验证流程，验证内容应包括措施是否按计划实施、实施后风险是否降至可接受水平、是否产生新的风险等；
d） 管控措施效果验证结果的记录和归档；
e） 对验证发现的不符合项自动纳入隐患排查治理流程。

5.3.6 风险管控措施的评估和优化应包括以下内容：

a） 实施前的可行性、有效性评估；

b） 实施后的效果再评估；
c） 失效时的重新评估和方案调整。

5.4 风险预警设计

5.4.1 风险预警功能模块应对工业生产过程中异常状态或潜在风险进行实时监测和提前预警。系统应支持基于监测数据、业务数据及人工数据的预警分析。

5.4.2 预警阈值应按风险程度设置差异化阈值，对于较高风险参数应设置多级阈值。

5.4.3 预警规则应基于风险辨识与评估结果设定，并结合企业风险承受能力和系统的历史数据进行修改。

5.4.4 对于涉及重大危险源的监控场景，系统的数据分析与预警功能应满足AQ 3035中关于故障诊断和事故预警的要求，根据监控数据及时发出预警信息。

5.4.5 系统应支持多级预警通知机制的设计，根据预警等级自动匹配相应的通知方式和通知对象。

5.4.5.1 预警通知方式宜包括以下内容：

a） 系统消息；
b） 短信；
c） 邮件；
d） 移动端推送；
e） 大屏弹窗；
f） 声光报警等。

5.4.5.2 预警通知对象应包括：

a） 岗位操作人员；
b） 现场管理人员；
c） 安全管理部门负责人；
d） 企业主要负责人等。

5.4.6 预警处置的闭环管理要求如下：

a） 接收确认信息；
b） 根据预警类型和等级将处置任务分配给相应的责任人员；
c） 对处置措施、时间、人员和结果等信息的在线记录；
d） 反馈和审核预警处置结果；
e） 自动上报提醒预警处置超期，对未及时处置的预警信息逐级上报至更高层级的管理人员。

6 系统支撑设计

6.1 数据安全

6.1.1 系统应具备数据安全保护能力，风险管控数据不应被泄露和篡改。

6.1.2 风险管控数据的分类分级可参照YD/T 4981的框架，根据数据的安全影响进行识别和分类。

6.1.3 数据访问控制机制应基于角色的访问控制（RBAC）机制实现对不同用户的数据访问权限管理。

6.1.4 应对风险管控系统中的重要数据在传输和存储过程中应采取加密保护措施。

6.1.5 操作日志审计功能应对所有数据访问和关键操作行为进行记录，日志记录应包括操作时间、操作人、操作内容、操作结果等信息。

6.1.6 应对风险管控数据进行定期备份，并具备在数据丢失或损坏时进行恢复的能力。备份数据应异地存储或与生产环境物理隔离。

6.1.7 数据安全设计应符合YD/T 4982的规定；涉及工业控制系统相关场景时，还应符合GB/T 41269的要求。

6.2 运行维护

6.2.1 具备运维管理功能应支持对风险管控系统的日常运行状态进行监控和管理。运维管理功能应包括系统运行监控、性能监测、故障告警、日志管理等基本模块。

6.2.2 应对风险辨识、评估、管控和预警等功能的运行效果进行周期性评估，建立定期评审机制。评审周期宜根据实际情况确定，一般不宜超过一年，评审内容应包括风险辨识的全面性、风险评估的准确性、管控措施的有效性、预警响应的及时性等。

6.2.3 统计分析生成多维度统计报表，为系统优化和改进提供数据支撑。

6.2.4 系统版本应进行定期升级管理，对系统功能更新和缺陷修复进行统一管理。系统升级前应进行测试验证。

6.2.5 可收集对系统功能、界面、性能等方面的意见和建议。