ICS 25.040.40
N 10

中华人民共和国国家标准

GB/T 38129—2019

智能工厂　安全控制要求

Smart factory—Safety and security control requirements

2019-10-18 发布　　2020-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、浙江中控技术股份有限公司、中国科学院沈阳自动化研究所、中国石油化工股份有限公司青岛安全工程研究院、霍尼韦尔(中国)有限公司、北京市劳动保护科学研究所、江苏省电子信息产品质量监督检验研究院、深圳市智瑞华科技有限公司、中国电力工程顾问集团华北电力设计院有限公司、清华大学、华中科技大学、北京康吉森技术有限公司、菲尼克斯(南京)智能制造技术工程有限公司、北京广利核系统工程有限公司。

本标准主要起草人:孟邹清、裘坤、徐皑冬、张占峰、靳江红、李玉明、张亚彬、马欣欣、史学玲、王敏良、任军民、赵劲松、周纯杰、周有铮、闫炳均、杨明、江国进、朱杰、朱明露、王璐、姜巍巍、张卫华、李荣强、李传坤、王刚、郭苗、柳晓菁。

引　言

智能工厂是智能制造的核心单元，涉及领域广泛，类型复杂多样。智能化技术给制造业带来难得发展机遇，使采用先进的技术手段进行工厂安全风险管控成为可能；但同时也使制造业面临着安全方面的挑战。

一方面，针对工业企业普遍存在的培训管理不认真、设备管理混乱、现场作业不规范、安全措施不充分、隐患排查不彻底、应急预案不完备、安全检查不到位、安全责任不落实等安全风险管控现状，通过物联网系统的透彻的感知、广泛的互联互通和深入的智能化，把健康、安全和环境管理的触角延伸到“人员的不安全行为或状态，物的不安全状态，工艺过程的不安全运行，机器或设备的不安全运转，环境的不安全状态”的实时管控层面，实现高危环境下的健康、安全和环境的全面感知、智能分析和即时控制管理；通过计算机软硬件技术和数据挖掘、智能分析技术的有机融合，构建制度化、精细化和流程化管理机制，控制安全管理风险漏洞，实现 PDCA（计划-实施-检查-对策）的循环优化。

另一方面，针对信息孤岛被打破后，生产现场的各类设备、系统安全防护能力不足的现状，通过采用技术和管理的手段，规范智能工厂的信息安全防护措施（如：防火墙、网闸等），建立信息安全纵深防御系统，实现信息安全风险的管控，构建信息资源的安全环境。

本标准：

a）　是一个通用基础标准，并适用于智能工厂的安全控制；

b）　提出智能工厂安全控制模型作为技术框架，覆盖智能工厂安全控制所必需的活动；

c）　提出需要满足智能工厂要求的安保策略或安保服务的开发、实现、维护和运行的要求，包括防止未经批准人员损害智能工厂的安全功能和对其产生不利影响的预防措施。

智能工厂　安全控制要求

1　范围

本标准规定了智能工厂安全控制的一般要求，人员安全管控、物料安全管控、过程安全管控、设备安全管控、环境安全管控及信息安全管控等方面的基本要求。

本标准适用于工程设计方、设备生产商、系统集成商、用户以及评估机构等进行智能工厂安全控制规划、设计、实施、验收与运行维护等阶段。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2017　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、硬件和软件要求

GB 50493　石油化工可燃气体和有毒气体检测报警设计规范

3　术语、定义和缩略语

3.1　术语和定义

GB/T 20438.4—2017 和 GB/T 21109.1 界定的以及下列术语和定义适用于本文件。

3.1.1

智能工厂　smart factory

在数字化工厂的基础上，利用物联网技术和监控技术加强信息管理和服务，提高生产过程可控性、减少生产线人工干预，以及合理计划排程。同时集智能手段和智能系统等新兴技术于一体，构建高效、节能、绿色、环保、舒适的人性化工厂。

3.1.2

功能安全　functional safety

整体安全中与 EUC 和 EUC 控制系统相关的部分，取决于 E/E/PE 安全相关系统和其他风险降低措施正确执行其功能。

[GB/T 20438.4—2017，定义 3.1.12]

3.1.3

安全相关系统　safety-related system

同时满足以下两项要求的系统：

——执行要求的安全功能足以实现或保持 EUC 的安全状态；

——自身或与其他 E/E/PE 安全相关系统、其他风险降低措施一起，能够实现要求的安全功能所需要的安全完整性。

注：改写 GB/T 20438.4—2017，定义 3.4.1。

3.1.4

安全功能　safety function

针对特定的危险事件，为实现或保持 EUC 的安全状态，由 E/E/PE 安全相关系统或其他风险降低措施实现的功能。

示例：安全功能的例子包括：

——在要求时执行的功能，作为一种主动行动以避免危险状况（如关闭电机）；

——采取预防行为的功能（如防止马达启动）。

[GB/T 20438.4—2017，定义 3.5.1]

3.1.5

安全完整性　safety integrity

在规定的时间段内和规定的条件下，安全相关系统成功执行规定的安全功能的概率。

注 1：安全完整性越高，安全相关系统在要求时未能执行规定的安全功能或未能实现规定的状态的概率就越低。

注 2：有 4 个安全完整性等级（见 3.5.8）。

注 3：在确定安全完整性时，宜包括所有导致非安全状态的失效原因（随机硬件失效和系统性失效），如硬件失效、软件导致的失效和电磁干扰导致的失效。某些类型的失效，尤其是随机硬件失效，可以用危险失效模式下的平均失效频率或安全相关保护系统未能在要求时动作的概率来量化，但是安全完整性还取决于许多不能精确量化只可定性考虑的因素。

注 4：安全完整性由硬件安全完整性（见 3.5.7）和系统性安全完整性（见 3.5.6）构成。

注 5：本定义针对安全相关系统执行安全功能的可靠性（见 IEV 191-12-01 可靠性的定义）。

[GB/T 20438.4—2017，定义 3.5.4]

3.1.6

安全完整性等级　safety integrity level

一种离散的等级（四个可能等级之一），对应安全完整性量值的范围。

注：改写 GB/T 20438.4—2017，定义 3.5.8。

3.1.7

信息安全　security

一种描述系统特性的术语，满足：

a）　保护系统所采取的措施；

b）　由建立和维护保护系统的措施而产生的系统状态；

c）　能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态；

d）　基于计算机系统的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统能力，却保证授权人员和系统不被阻止；

e）　防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。

注 1：措施可以是与物理信息安全（控制物理访问计算机的资产）或者逻辑信息安全（登录给定系统和应用的能力）相关的控制手段。

注 2：改写 IEC/TS 62443-1-1:2009，定义 3.2.99。

3.1.8

安全关键　safety critical

一种表示某一状态、事件、动作、过程或产品的正确识别和控制、适当的性能或容差对保证产品安全工作和使用来说是关键的描述性术语。

示例：如安全关键的功能、安全关键的部件等。

3.1.9

网络安全　cybersecurity

用于防止关键系统或者信息类资产的非授权使用、拒绝服务、修改、泄露、财政损失和系统损害的

行为。

注：目标是降低风险，这些风险包括人身伤害、威胁公共健康、丧失公众或者消费者信任度、泄露敏感资产、不能保护商业资产，或者违背法规。这些概念适用于生产过程的任何系统，包括单机的和网络的设备。系统间的通信可以通过内部报文或者通过任何的操作员或机器接口，以便认证、操作、控制，或和任意的控制系统交换数据。计算机安全包括标识、认证、问责制、授权、可用性和隐私。

[IEC/TS 62443-1-1:2009，定义 3.2.36]

3.2 缩略语

下列缩略语适用于本文件。

CRM：客户关系管理(Customer Relationship Management)

E/E/PE：电气/电子/可编程电子(Electrical/Electronic/Programmable Electronic)

ERP：企业资源计划(Enterprise Resource Planning)

EUC：受控设备(Equipment Under Control)

GDS：气体检测系统(Gas Detection System)

IDS：入侵检测系统(Intrusion Detection System)

MES：制造执行系统(Manufacturing Execution System)

MRP：物资需求计划(Material Requirement Planning)

MSDS：化学品安全技术说明书(Material Safety Data Sheet)

NOX：氮氧化物(Nitrogen Oxide)

OTS：操作员培训系统(Operator Training System)

RFID：射频识别(Radio Frequency Identification)

SCM：供应链管理(Supply Chain Management)

USB：通用串行总线(Universal Serial Bus)

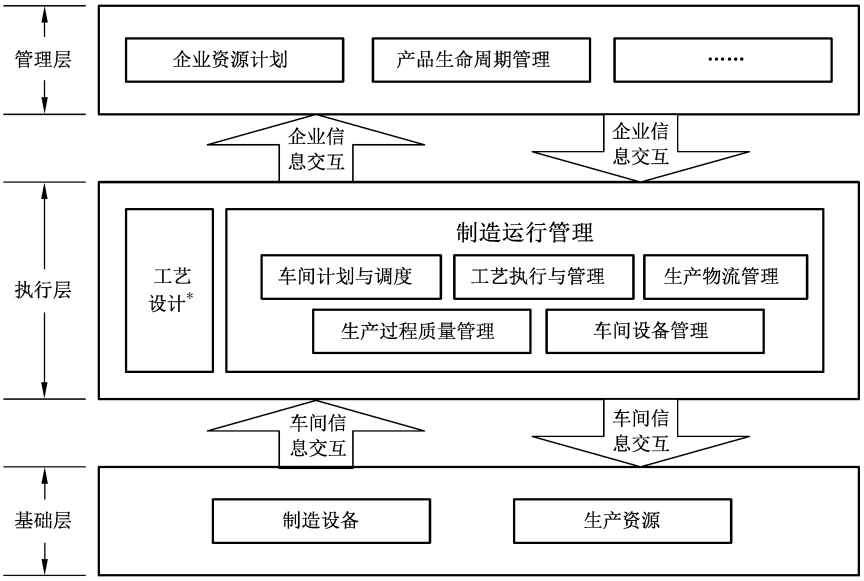
VOC：挥发性有机化合物(Volatile Organic Compounds)

4 一般要求

4.1 智能工厂层次模型

智能工厂按照功能可分为三个层次：管理层、执行层、基础层。其中管理层是面向生产制造类工厂或企业的综合经营管理；执行层面向生产制造车间；基础层则包括车间内具体承担制造任务的设备及其附属设施。智能工厂的层次模型如图 1 所示。

注：本标准参考了 GB/T 37393—2019 中对企业/车间的功能层次划分，同时参考了 GB/T 25485—2010 中制造类企业功能层次模型，结合本标准的实际情况，给出了该功能层次模型的描述。



* 数字化车间/智能工厂可选功能

图 1 智能工厂的层次模型

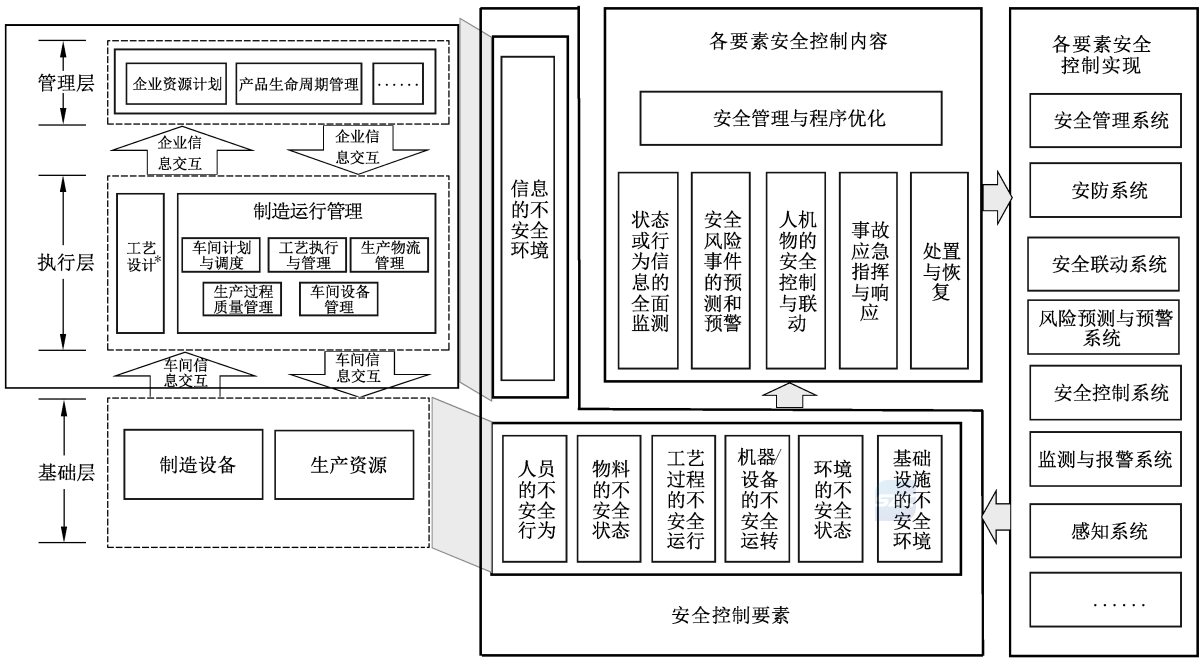
基础层包括数字化车间中生产制造所需要的各种制造设备及生产资源，其中制造设备承担执行生产、检验、物料运送等任务，大量采用数字化设备，可自动进行信息的采集或指令执行；生产资源是生产用到的物料、托盘、工装辅具、人、传感器等，本身不具备数字化通信能力，但可借助条码、RFID 等技术进行标识，参与生产过程并通过其数字化标识与系统进行自动或半自动交互。

执行层介于管理层和基础层之间，定义了为了实现生产出最终产品的工作流的活动。包括记录维护和过程协调等活动。主要包括车间计划与调度、工艺执行与管理、生产物流管理、生产过程质量管理、车间设备管理等，对生产过程中的各类业务、活动或相关资产进行管理，实现车间生产制造过程的数字化、精益化及透明化。可以通过 MES 实现这些功能。

管理层定义了制造型企业管理所需要的相关业务类活动。包括管理企业中的各种资源、管理企业的销售和服务、制定生产计划、确定库存水平，以及确保物料能按时传送到正确的地点进行生产等。通常会选用 ERP(或 MRP II)、SCM、CRM 等系统。

4.2 智能工厂安全控制模型

智能工厂的安全控制，涵盖智能工厂的三个层级，即基础层、执行层和管理层。其中，基础层的安全风险要素主要包括人员的不安全行为或状态，物料的不安全状态，工艺过程的不安全运行，机器或设备的不安全运转，环境的不安全状态，信息资源的不安全环境等几个方面；执行层和管理层的安全风险要素主要包括信息资源的不安全环境。每一类安全风险要素，又分别有各自的安全控制内容和实现的技术手段。最终实现人员、物料、过程、设备、环境、信息等六类安全风险要素的智能化管控，将智能工厂的风险控制在可接受范围，保障智能工厂的安全运行。智能工厂的安全控制模型，见图 2。



* 数字化车间/智能工厂可选功能

图 2 智能工厂安全控制模型

4.3 一般要求

4.3.1 应设立智能工厂安全管理机构，统一负责智能工厂的人员、物料、过程、设备、环境、信息安全的管控。

4.3.2 应全面梳理生产运营过程中潜在的风险要素，面向对象进行风险界定、辨识、评估、控制和管理。

4.3.3 应制定风险管理准则，针对不可接受的风险场景，制定风险控制的方法和手段。

4.3.4 应制定风险管控流程，明确所有风险管控相关岗位职责和要求。完善各项安全管理制度，如生产责任制、安全操作规程、应急预案体系等。

4.3.5 应合理利用物联网、计算机软硬件技术和数据挖掘智能分析技术的有机融合机制，对风险进行感知、传输、分析处理、预警响应、应急预案触发、善后处理、总结改进提高，实现生产过程中人员、物料、过程、设备、环境、信息等六类安全风险要素的智能化管控。

4.3.6 应对用于智能工厂安全控制的装置和系统（含感知、监测与报警、安全控制、风险预测与预警、安全联动、安防和安全管理系统）进行评估和测试，验证其安全完整性水平和安全防护能力，以确定安全控制有效性。

5 人员安全管控

5.1 人员能力与资质

5.1.1 人员安全培训应关注于训练人员如何以安全、正确的方式进行作业，包括对安全风险要素的理解，对智能化、数字化设备的熟悉和掌握等。应对培训内容、培训成效、相关人员作业资质等信息进行详细的电子记录。

注：人员能力体现在技术、经验和资质等几个方面，对人员的管控实质上是通过技术与管理手段提高人员能力和规范人员行为，进而保障人员的安全。

5.1.2 宜根据培训需求使用仿真模拟系统针对不同的场景来训练人员的能力，可配合采用 AR/VR 技术、实操、体感等，创建更为逼真的沉浸式培训环境。

注：基于仿真模拟技术的培训，例如：采用 OTS，在计算机上仿真模拟化工、石化或炼油等行业各流程的真实生产过程，建立对应的虚拟工厂，包含其生产过程及其控制逻辑。在此基础上，实现对工厂过程和控制逻辑的模拟、调整和培训。

5.1.3 现场作业人员应具备相关的作业资质，人员资质应能够通过技术手段（如指纹、虹膜等）与人员个体进行绑定以保证唯一性。

5.1.4 人员培训和资质信息应通过移动设备进行在线查询，以确保进行作业的人员满足该区域的安全培训、资质方面的要求。

5.2 现场安全防护装备

5.2.1 现场安全防护装备包括但不限于个人防护装备、现场安全装备、便携式气体探测器，这些装备的配置应满足国家法律法规和企业规划的要求。

5.2.2 个体防护装备包括但不限于安全帽、安全带、防噪音耳机、护目镜、口罩、呼吸器、防护服等。个人防护装备宜为可穿戴设备，并可通过扫码、无线 ID 识别等技术手段对设备的类型和功能进行识别。

5.2.3 现场安全装备包括但不限于灭火器、灭火毯等，应配置相应的编码，支持对设备类型和功能的扫码识别。

5.3 人员安全管理系统

5.3.1 宜建立人员安全管理系统，该系统至少应具备以下的功能：

——人员培训记录、资质等信息；

——防护装备台账；

——防护装备的维护计划和检验记录；

——对上述信息进行实时检索的能力；

——支持多用户同时访问；

——用户权限管理。

5.3.2 系统宜支持云平台，系统内的信息应支持实时检索。

5.3.3 系统应支持项目管理模式，对项目下涉及的人员能力、资质、防护装备等信息实时搜集并以默认或定制的形式呈现，应支持对项目合规性的监督和检查。

5.3.4 系统应识别对特种作业人员的资质和防护装备配备不合规的情况并进行报警。

5.3.5 系统应具有实时显示现场人员位置、环境参数、人员生命体征、人员跌落等信息的功能。

5.4 人员定位

5.4.1 作业现场应配置适当的设备来构建临时或永久性的无线通信网络，比如卫星、无线局域网等。

5.4.2 作业人员在现场的物理位置可以通过卫星、RFID、无线局域网，蓝牙或无线移动网络等技术进行定位，定位精度应满足具体应用要求。

5.4.3 作业人员的位置、生命体征等信息应可以在人员安全管理系统或其他终端设备上实时显示。

5.5 危险作业人员管理

5.5.1 应针对受限空间、动火作业等危险作业的类型和作业情况选择和设计合适的探测技术和设备。

5.5.2 作业人员在开展危险作业之前，应持作业证，熟悉操作规程。应通过移动终端设备对作业人员的资质、防护装备配置以及装备的有效性等进行确认，确保合规。

5.5.3 开展危险作业的人员应配备相应的安全防护装备，实现对有毒有害气体和人员的生命体征、人

员跌倒等的实时监控;必要时,还应配备通信设备保证作业人员与外部通信的通畅。应配置针对特定危险作业环境下进行安全防护装备的匹配性检查和报警能力。

5.5.4 危险作业时应配置相应的救助设备,并且可以通过现场终端设备随时进行检查和确认。

5.5.5 在发生异常时,应根据应急响应流程予以施救,应急响应流程应支持在移动设备上的调用和显示。

6 物料安全管控

6.1 一般要求

6.1.1 智能工厂应建立物料安全管理系统,生产用所有物料均应纳入物料安全管理系统中。

6.1.2 物料安全管理系统应对危险化学品物料的购买、存贮、转运、使用、废弃的流程等在规范的基础上进行统一管理,实现电子化的记录、追踪和追溯。危险化学品物料管理模块应包含危险化学品名称、MSDS、危险化学品混存性能互抵表、物料责任人、储存或使用场所、出入量等信息。

6.1.3 其他非危险化学品物料可结合企业实际情况记录物料名称、物料责任人、储存或使用场所、出入量等信息。

6.2 罐区

6.2.1 罐区应建立相对独立的物料安全管理子系统。该系统应包括储罐内安全监控装备及其连锁自动控制装备、重要机泵状态监控系统。

6.2.2 危险化学品物料罐区还应设置环境可燃、有毒气体监测报警系统和泄漏控制装备,储罐溢流自动防护系统、罐区气象监测、防雷和防静电装备,罐区火灾监控及报警装置,罐区视频监控、周界防范、门禁管理、巡检及定位管理等安全防范系统以及罐区应急处置决策系统。

注:对罐区溢流进行风险分析、确定储罐溢流自动防护系统的安全完整性等级、确定溢流保护报警液位,并采用适当的液位连续测量仪表(宜具有自检和报警功能)、逻辑解算器和执行机构来构成独立的罐区溢流自动防护系统。

6.3 仓库、储存室、气瓶间和储存柜

6.3.1 非储罐存储的物料应建立相对独立的物料安全管理子系统。所有非储罐储存的物料应采用RFID技术进行物料出入量记录、追踪和追溯。储存场所应设置环境温湿度监控系统。

6.3.2 危险化学品物料储存场所除应设置环境温湿度监控系统外,还应设置符合GB 50493要求的可燃、有毒气体浓度检测报警装置。气体声光报警控制器应设置在危险物料储存场所外并接至有人值守的值班室内。气体浓度检测报警装置应与防爆通风机联动。

6.3.3 应设置适当的物理安防措施。

6.4 重大危险源

罐区应建立相对独立的物料安全管理子系统。该系统应包括储罐内安全监控装备及其连锁自动控制装备、重要机泵状态监控系统。储罐区、库区和生产场所如构成重大危险源,还应设有相对独立的安全监控预警处置系统,系统中的设备应符合有关国家法规或标准的规定。同时满足以下条件:

a) 控制设备应设置在有人值班的房间或安全场所;

b) 系统报警等级的设置应同事故应急处置与救援相协调,不同级别的事故分别启动相对应的应急预案;

c) 对于容易发生燃烧、爆炸和毒物泄漏等事故的高度危险场所、远距离传输、移动监测、无人值守或其他不宜于采用有线数据传输的应用环境,宜选用无线传输技术与装备。

7 过程安全管控

7.1 过程安全管控流程

7.1.1 应统筹考虑智能工厂过程安全控制相关活动，定义智能工厂过程安全生命周期阶段以及各阶段相关内容和要求、责任人，并文档化。

7.1.2 宜采用统一的数字化管理平台对生命周期的过程活动进行记录、变更和管控。

7.2 危险识别

7.2.1 应对智能工厂生产过程及相关设备开展危险分析，识别危险和危险事件、导致危险事件的原因及其后果。

7.2.2 对于不同的应用场景，对危险源的危险特征要素应进行实时有效监控，并与预设的标准值进行比对，实现超限报警、反馈调节等功能；对设备的失效进行检测和记录，并统计设备的实际失效率数据。

7.2.3 应甄别人员活动信息，实现进入危险区域的预警、异常行为报警、异常状态报警等功能。

7.3 风险评估

7.3.1 应识别与危险事件相关的过程风险、风险降低和要达到必要的风险降低所需要的安全措施。

7.3.2 应实时采集危险状态下风险参数信息，对实际的过程风险进行监视和量化统计。

7.4 保护层

7.4.1 应设计基于保护层的风险降低措施，采用 E/E/PE 安全相关系统和其他风险降低措施，使过程安全风险达到可容忍的范围。

注：基于保护层的风险降低措施涵盖与过程安全相关的、由仪表系统实现的各种安全控制、报警以及安全连锁进行识别并确保其机械完整性，包括但不限于如安全报警、安全连锁、安全许可、GDS、紧急停车系统、安全控制等存在形式，而且这些存在形式并不一定要完全分离或独立存在。

7.4.2 应对实现风险降低的各类关键保护层措施进行监视，并与中高风险的危险场景进行关联，建立危险源风险等级与保护层降险等级之间的比对关系，监视关键危险源残余风险的实时动态变化情况。

7.5 安全相关报警管理系统

应设立安全相关的报警性能监视和运维系统，实时监视控制系统或安全系统层面与安全相关的报警的健康状态，提供报警操作的在线指导，帮助报警系统的维护决策。

注：报警管理参照相关国家标准，ANSI/ISA 18.2、EEMUA191 等标准，或最佳工程实践。

7.6 安全相关系统

7.6.1 应根据安全相关系统设计有关标准规范和规定，设计相应的安全相关系统。

7.6.2 应对安全相关系统的安全完整性等级进行全过程的动态监测。安全完整性监测针对执行安全功能的控制系统，应：

——关注并采集系统功能设置、失效模式、安全状态、操作模式、响应时间、设备状态、诊断及反馈、故障频率及响应等信息；

——提供在实际运行条件下安全完整性的可视化，监视随时间变化的安全完整性等级；

——与风险监视与预警单元信息交互，及时观察风险环境变化，评估风险状况，随时更新实际运行条件下的风险等级，实现风险可视化管理。

7.6.3 对于安全完整性降低的部件，应发出预警或报警，并与相关管理单元信息交互，提出预案。

7.7 运行维护要求

7.7.1 应编制运行维护规程，制定运行维护计划。

7.7.2 应依据预测性维护动态制定维护和测试活动，确认保护层风险减低措施，及安全相关系统运行是否正常。

7.7.3 应建立电子化运行维护日志，并开展安全审计。安全审计活动应包括：

——是否有新增危险源；

——危险源的风险评估是否准确；

——安全相关系统是否运行正常；

——其他保护层措施是否有效；

——运行维护是否符合运行维护规程；

——变更修改是否符合变更修改规程。

7.7.4 按时间编制智能工厂安全相关系统及其他保护层措施的运行和维护文档，应妥善保存并包括下列信息：

——功能安全审核和测试的结果；

——存在的问题、采取的纠正措施、纠正的结果、执行人的记录；

——向智能工厂安全相关系统及其他保护层措施发出要求的原因和时间，连同收到那些要求时安全相关系统的性能，以及日常维护中发现的故障等文档；

——智能工厂现场设备、控制系统及过程安全管理系统等安全相关系统所作修改的文档。

7.7.5 应对安全相关的控制、报警和连锁功能进行管理，保证其安全完整性要求。

7.8 变更和停用要求

7.8.1 应制定变更修改规程，防止人员进行未批准的变更。

7.8.2 安全相关系统及其他保护层措施的修改或变更应符合变更修改规程，并应按审批程序获得授权批准，并应保留变更记录。

7.8.3 在进行停用处置活动之前应进行影响分析，影响分析包括建议的停用处置活动对智能工厂的影响评估，影响分析还应考虑到相邻的工厂。评估应包括危险识别和风险评估，此分析应足以确定整体风险水平没有提升。

7.8.4 如果停用处置活动会对过程安全产生影响，应终止停用处置活动，增加必要的风险降低措施后，再重启停用处置活动。

7.9 过程安全管理系统

7.9.1 应配置过程安全管理系统，能够实时采集过程安全状态数据，提供过程安全监测和风险预警，提高过程安全管理可视化水平。

7.9.2 过程安全管理系统应跟踪并指导安全相关系统、其他技术的风险降低措施、备品备件及其检测维护工具等维护活动，从而保证这些资源在制造过程中的可用性；实现安全相关系统不同安全等级条件下的周期性维护、状态维护或故障检修维护的提醒（报警）及调度功能；建立维护事件或问题的历史信息库，以支持故障诊断。

注：过程安全管理系统设置具备全厂级集成的安全操作窗口（即，所有与操作安全相关的可度量的操作安全限值数据库），可实时、定量地识别当前安全状况与隐患，对超限指标进行报警和实时分析。

7.9.3 过程安全管理系统应跟踪并指导安全相关系统、其他技术的风险降低措施等的变更活动；建立变更活动历史信息库，以支持变更追溯；实现变更状态提醒，其他功能模块相关信息应随变更同步更新，可视需要采用实时同步或定期同步的方式。

7.9.4 过程安全管理系统应协助各级人员对过程风险进行处理，提供工作流程管理功能及跟踪反馈功能。

7.9.5 过程安全管理系统应具备对安全相关的操作日志、交接班等进行电子化的能力，规避人工记录的安全隐患。

8 设备安全管控

8.1 基本要求

8.1.1 应建立健全设备的操作、使用、维护规程，建立岗位责任制。设备的操作和维护人员应严格遵守设备操作、使用和维护规程。

8.1.2 对于动力、起重、运输、仪器仪表、压力容器等机械、电子、电气设备的设计、制造、使用、维护等，应符合国家相关标准要求，按照国家有关规定执行。

8.1.3 设备及其零部件，应有足够的强度、刚度、稳定性和可靠性；不应向工作场所和周边环境排放超过国家标准规定的有害物质，不应产生超过国家标准规定的噪声、振动、辐射和其他污染。对有可能产生的有害因素，应采取有效措施进行防护。

8.1.4 应在工艺流程中或生产设备上设置安全防护装置，防止在人的不安全行为发生后造成伤亡事故；当危险因素对人体的伤害与距离远近有关时，应采取安全距离防护措施，设置隔离标识，配置靠近报警，必要时设置连锁动作控制设备进入安全作业状态；应使用互锁装置强制发生作用；当其他方式无法消除危险因素时，应采取自动控制或紧急停止装置保障设备运行和人员财产安全。

8.1.5 安全关键设备应具有写保护功能和写保护指示，安全关键设备应具有防篡改功能并具有对外提供篡改报告的能力。

8.2 设备状态监测与故障诊断

8.2.1 应对安全关键设备配置在线监测系统。记录设备运行的各种参数（如振动、温度、压力、流量、辐射、噪声等），使设备始终处于被监控状态。

8.2.2 应对安全关键设备配置故障分析和诊断系统。广泛采集并记录故障直接信息和关联信息，辅助或智能判断故障现象，实现故障报警；结合诊断对象的历史状况，分析判断故障部位、原因，确定必要的维修策略和适宜的修理时间。可根据需求为设备诊断系统配置远程功能。

注：安全管理的长期目标是建立以设备健康状态和工艺过程绩效为中心的更高级别的实时分析及远程诊断平台，通过互联网技术把智能仪表、设备的和工艺过程的性能表现数据组合在单一的健康监视中心进行监视，实现对关键设备的全方位的、智能化的性能监视和预测性的维护。

8.2.3 对安全关键设备宜根据需要配置预测性维护系统。

8.2.4 应对工厂重要信息，如重大设备故障或报警等信息，配置实时推送到移动设备的功能。

8.3 设备安全管理系统

8.3.1 应对安全相关设备建立设备全生命周期检维修管理系统。覆盖设备全生命周期的检维修记录、费用预算管理等。

8.3.2 应对安全相关设备建立设备动态关联系统。设备状态随巡检、盘点等业务数据动态更新。

8.3.3 应建立备品备件管理系统。备品备件信息与设备关联，使用记录清晰可查。

8.3.4 应建立设备安全完整性分析系统。多维度分析设备状态数据、检维修信息、备品备件质量及使用情况、人员配置、运行维护费用等，关联安全完整性指标，实现综合分析、预警和管理优化。

8.4 设备腐蚀监控

宜针对生产设备的腐蚀情况进行监测，通过智能技术（如传感技术、预测技术）掌握设备腐蚀的动态

变化趋势，避免因腐蚀造成设备损坏进而引发重大的安全事故或环境污染事故。

9 环境安全管控

9.1 一般要求

9.1.1 应识别智能工厂的运行及维护过程中能够控制和能够施加影响的环境因素及其相关的环境影响。应制定统一的评价准则，识别重要环境因素。包括但不限于废水、废气、噪声、固废、资源、能源消耗、化学品使用、相关方、产品等。

9.1.2 应根据识别的环境因素，确定对应的环境目标，并应采取措施实现对应的环境目标。

9.1.3 应对重要环境因素进行自动的监视和报警，如果该环境因素可被控制，应设计控制方案。

9.2 作业场所

9.2.1 应对智能工厂各类作业场所的环境安全因素进行安全管控，包括但不限于照明、温度、湿度、噪声与振动、辐射等。

9.2.2 应为作业环境提供高质量的照明条件，确定恰当的视野范围宽度、照度，避免眩光和太暗的灯光。

9.2.3 应依据作业场所环境要求对温湿度自动检测、调节、显示并超限报警。

9.2.4 应依据作业场所环境要求对振动、噪声等自动检测、显示并超限报警。

9.2.5 接触限值及屏蔽措施应满足国家或企业规范要求，使用个体防护设备的应满足 5.2 的要求。

9.3 生产设备

应对智能工厂各类生产作业设备的环境安全因素进行识别和管控。生产设备的环境安全管控要求见 8.1.3。

9.4 环境监测与管理

应建立环境安全监测管理系统。对粉尘、烟气、NOX、VOC、雾尘、雾、蒸气、气体、气溶胶、烟气等有害环境因素进行自动化监测和管理，设置现场实时显示、趋势报警、超限报警、必要时的自动控制调节、处置决策、环境风险集中管理等功能。

针对危化品存储罐区，宜设置自动防渗漏系统，对罐底的土壤和附近水系进行实时监测。

9.5 环境检查与管理

应建立环境安全检查管理系统。对工作设置，平面布置，建筑标准，车间环境，厂内运输，原料、材料与燃料，工作操作防护，生产设备，防灾设施等作业环境布设状况、作业环境条件状态和作业环境防护设施状态进行视频监视、智能巡检，设置现场状态实时显示、异常报警、处置决策支持、协同信息交互、环境风险集中管理等功能。

10 信息安全管控

10.1 物理访问控制要求

10.1.1 应对智能工厂出入口进出的人员进行管控、鉴别和电子化记录，以实现对人员的活动路径进行识别、追踪与追溯。

10.1.2 应对智能工厂按照安全管控级别进行区域划分和分级管理，必要时，区域和区域之间应物理

隔离。

10.1.3 应对重要区域进出的人员进行管控、鉴别和电子化记录。

10.1.4 应全程陪同对重要区域访问的外部人员。

10.1.5 应限制外部人员携带可能导致泄密的电子设备或其他物品。

10.1.6 应制定规章制度限制内部人员携带可能导致泄密的物品。

10.1.7 应进行物理视频监控。

10.2 信息安全管理要求

10.2.1 一般要求

智能工厂应依据业务要求和相关法律法规建立与之相适应的信息安全管理制度，并采取有效的措施进行评估、分析和改进，以满足信息安全管理的要求。

10.2.2 安全管理制度

10.2.2.1 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

10.2.2.2 应对安全管理活动中的各类管理内容建立安全管理制度。

10.2.2.3 应对要求管理人员或操作人员执行的日常管理操作建立操作规程。

10.2.2.4 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

10.2.3 安全管理机构

10.2.3.1 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

10.2.3.2 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

10.2.3.3 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。

10.2.3.4 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

10.2.4 资产管理

10.2.4.1 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

10.2.4.2 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

10.2.4.3 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。

10.2.4.4 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

10.2.4.5 应对网络的安全性和可能存在的风险定期进行评估（如年度评估），并采取必要的补救措施。

10.2.5 供应链管理

10.2.5.1 在选择工厂规划、设计、建设、运维或评估等服务商时，应以合同等方式明确服务商应承担的信息安全责任和义务。

10.2.5.2 应以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。

10.3 安全技术要求

10.3.1 边界安全防护

10.3.1.1 工厂的开发、测试和生产环境应执行不同的安全控制措施，可采用物理隔离、网络逻辑隔离等

方式进行隔离。

10.3.1.2 应通过网络边界防护设备对工厂网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的车间网络与互联网连接。

10.3.1.3 应通过工业防火墙、网闸等防护设备对工厂网络安全区域之间进行逻辑隔离安全防护。

10.3.1.4 对网络结构、区域划分等进行变更时应进行风险评估。

10.3.1.5 应对使用 USB 端口的移动存储设备进行必要的检测和隔离措施，阻止病毒或恶意软件的传播，防止信息的泄漏。

10.3.2 网络安全

10.3.2.1 结构安全

应将生产系统和非生产系统网络进行逻辑分区。

10.3.2.2 访问控制

访问控制包括：

——应保证设备的业务能力具有冗余空间，满足业务高峰期需要；

——应在网络边界部署访问控制设备，启用访问控制功能；

——应对网络数据流进行控制，提供例外允许网络数据流（也称为拒绝所有，允许例外）的能力。

10.3.2.3 异常监测

异常检测包括：

——应在交换机处监视车间的网络流量、连接数等网络资源信息，并根据安全策略要求对流量、连接数进行限制；

——应在网络中设置入侵检测系统，能够在监视到攻击行为时记录并提供报警；

——应监视和控制经由不可信网络对系统的访问。

注：IDS 是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处在于，IDS 是一种积极主动的安全防护技术。

10.3.2.4 流量审计

流量审计包括：

——应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

——应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；

——应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。

10.3.2.5 网络边界检测

网络边界检测包括：

——应对非授权设备私自连到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

——应对内部网络用户私自连到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

10.3.3 主机安全

10.3.3.1 身份鉴别

身份鉴别包括：

——应对用户身份进行鉴别和认证，操作人员需要使用用户名和密码才可以操作系统；

——应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
——应对单个账户的多重并发会话进行限制。

10.3.3.2 权限管理

权限管理包括：
——应提供统一的账号管理功能，包括账号的创建、激活、修改、禁用和移除账号的能力；
——应在上位机安装白名单管理可信的软件进程；
——应对上位机限制代码和数据传入传出便携和移动设备；
——应对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码来源要求适当的鉴别和授权；监视移动代码的使用。

10.3.3.3 系统容错能力

系统容错能力包括：
——应提供数据有效性校验功能，保证输入的数据格式或长度符合系统设定的要求；
——应提供自动保护的功能，当故障发生时自动保护当前所有状态。

10.3.3.4 病毒及恶意代码防护

应采取经验证的杀毒软件，并定期更新相关病毒库。

10.3.3.5 补丁管理

宜及时更新经过控制厂商验证的操作系统或第三方补丁，确保已暴露的漏洞尽早被修复。

10.3.4 数据安全

10.3.4.1 应对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。
10.3.4.2 应对关键业务数据，如工艺参数、配置文件、设备运行数据、生产数据、控制指令等进行定期备份。
10.3.4.3 应对测试数据，包括安全评估数据、现场组态开发数据、系统联调数据、现场变更测试数据、应急演练数据等进行保护，如签订保密协议、回收测试数据等。

10.3.5 安全监测和应急预案演练

10.3.5.1 应在智能工厂网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。并对相关漏洞、异常行为进行分析，提供改进措施。
10.3.5.2 应在重要车间设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。
10.3.5.3 应制定安全事件应急响应预案，当遭受安全威胁导致车间出现异常或故障时，应立即采取紧急防护措施。
10.3.5.4 应定期对智能工厂的应急响应预案进行演练，必要时对应急响应预案进行修订。

参 考 文 献

[1] GB 6944—2012 危险货物分类和品名编号
[2] GB 17914—2013 易燃易爆性商品储存养护技术条件
[3] GB 17916—2013 毒害性商品储存养护技术条件
[4] GB/T 25485—2010 工业自动化系统与集成 制造执行系统功能体系结构
[5] GB 28644.1—2012 危险货物例外数量及包装要求
[6] GB 28644.2—2012 危险货物有限数量及包装要求
[7] GB/T 37393—2019 数字化车间 通用技术要求
[8] AQ 3035—2010 危险化学品重大危险源 安全监控通用技术规范
[9] AQ 3036—2010 危险化学品重大危险源 罐区现场安全监控装备设置规范
[10] IEC/TS 62443-1-1:2009 Industrial communication networks—Network and system security—Part 1-1:Terminology,concepts and models
[11] API 2350 Overfill Protection for Storage Tanks in Petroleum Facilities
[12] ANSI/ISA 18.2—2016 Management of alarm systems for the process industries
[13] EEMUA 191 Alarm Systems—A guide to design,management and Procurement