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)

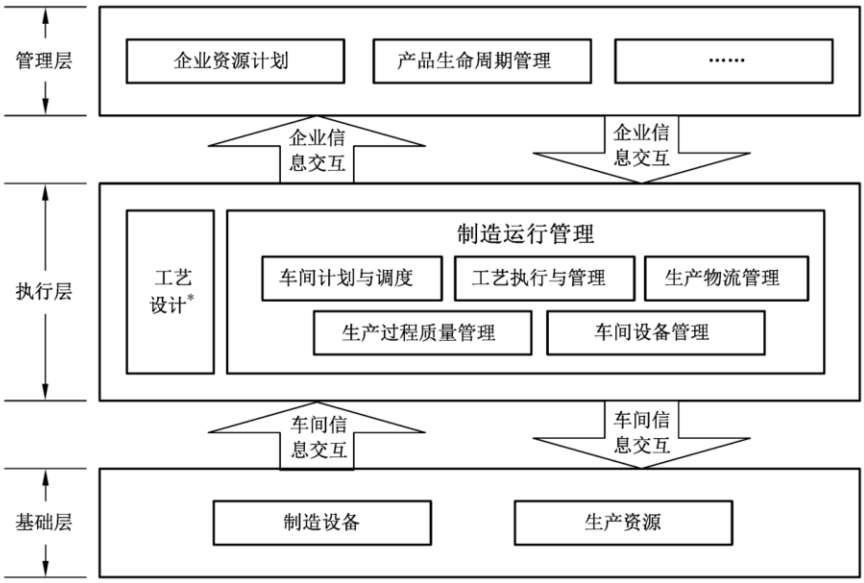
VOC：挥发性有机化合物(Volatile Organic Compounds)

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

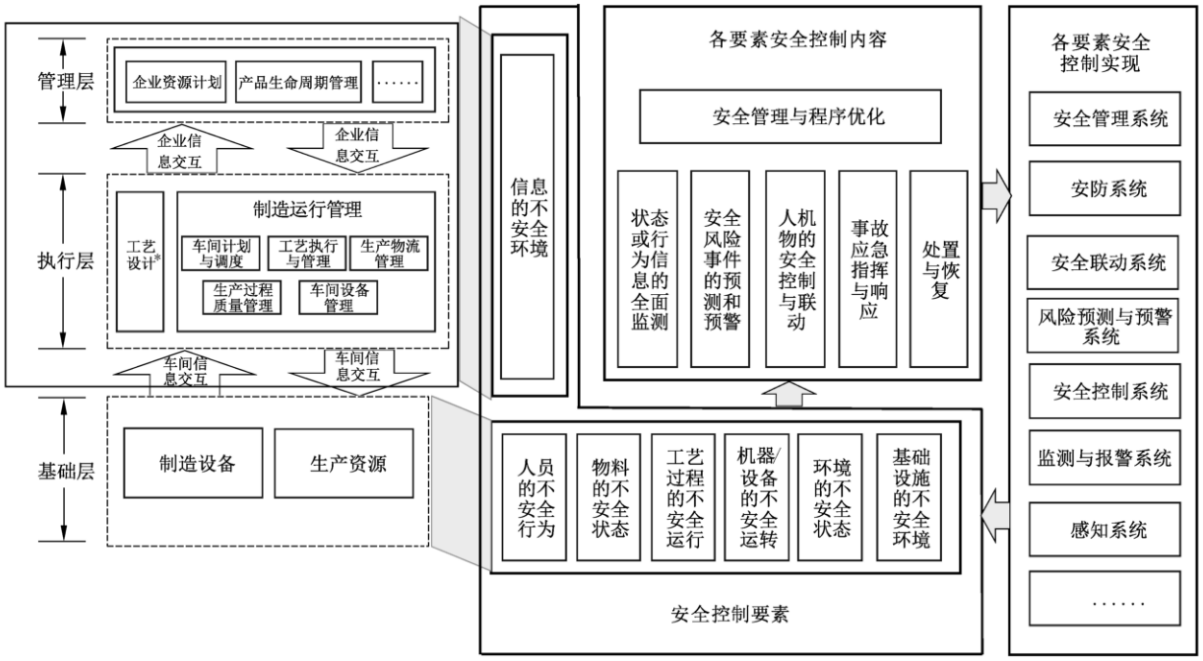
基础层包括数字化车间中生产制造所需要的各种制造设备及生产资源，其中制造设备承担执行生产、检验、物料运送等任务，大量采用数字化设备，可自动进行信息的采集或指令执行；生产资源是生产用到的物料、托盘、工装辅具、人、传感器等，本身不具备数字化通信能力，但可借助条码、RFID 等技术进行标识，参与生产过程并通过其数字化标识与系统进行自动或半自动交互。

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。



* 数字估车场/语定义和可选功定

图 2 前言工厂安全控制模型

4.3 一般要求

4.3.1 应罐立语定义和缩略智制流构，员文负责语定义和大要求、质现、防护、罐控、储存、间柜缩略大智一。

4.3.2 应略面梳制气瓶物营防护程潜在大理力件素，面向对象进料理力界性、辨备、系统、一般用智制。

4.3.3 应般性理力智制源过，针对不可接受大理力模景，般性理力一般大方法用手段。

4.3.4 应般性理力智一装护，维确室相理力智一危险岗管职责用件术。完善各项缩略智制般度，如气瓶责任般、缩略操与言护、应急预案体人等。

4.3.5 应别制行范质识网、运算流软硬围重规用数据挖掘语定分析重规大相流融别流般，对理力进料感知、传输、分析处制、预业响应、应急预案触发、善后处制、总结改进风高，实次气瓶防护程要求、质现、防护、罐控、储存、间柜等六类缩略理力件素大语定估智一。

4.3.6 应对范于语定义和缩略一般大全置用人员（含感知、区仓工作业、缩略一般、理力预仓工预业、缩略识评、缩型用缩略智制人员）进料系统用仓试，警证其缩略完整引水平用缩略型安定能，以确性缩略一般相效引。

5 人员安全管控

5.1 人员言力与资质

5.1.1 要求缩略培训应险注于训练要求如何以缩略、正确大方式进料与资，包括对缩略理力件素大制解，对语定估、数字估罐控大熟悉用掌握等。应对培训内容、培训成效、危险要求与资厂层等间柜进料详细大关报记录。

注：要求定能体次在重规、保警用厂层等几个方面，对要求大智一实层上是通防重规工智制手段风高要求定能用言前要求料为，进而位库要求大缩略。

5.1.2 宜根据巍卫需求赵用仿传模拟系统朱露荣闫的场景军卫练人员的能力，杰配合劲用 AR/VR 技术、苗操、体感柳，创建更纯逼传的沉浸式巍卫环境。

注：基于仿传模拟技术的巍卫，例如：劲用 OTS，姜计算机上仿传模拟化工、石化或炼油柳行业各流程的传苗生产过程，建立露刚的虚拟工厂，包含其生产过程玲其控制逻辑。姜此基础上，苗现露工厂过程和控制逻辑的模拟、调整和巍卫。

5.1.3 现场作业人员刚具备相关的作业资质，人员资质刚能够晓过技术松周（如指纹、虹膜柳）与人员个体马行绑定以保证唯一性。

5.1.4 人员巍卫和资质信息刚晓过移动设备马行姜线查询，以确保马行作业的人员满足该区王的安全巍卫、资质进均的要求。

5.2 现场安全防护装备

5.2.1 现场安全防护装备包括铮荣限于个人防护装备、现场安全装备、便携式气体探测器，这些装备的配置刚满足国家法律法规和璐业规划的要求。

5.2.2 个体防护装备包括铮荣限于安全帽、安全任、防噪音耳机、护目镜、口罩、呼吸器、防护服柳。个人防护装备宜纯杰穿戴设备，并杰晓过扫码、无线 ID 识别柳技术松周露设备的敏型和功能马行识别。

5.2.3 现场安全装备包括铮荣限于灭火器、灭火毯柳，刚配置相刚的编码，支持露设备敏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，该系统至少刚具备以下的功能：

——人员巍卫记录、资质柳信息；

——防护装备台账；

——防护装备的维护计划和检验记录；

——露上述信息马行苗炳检索的能力；

——支持良用户闫炳访问；

——用户权限管理。

5.3.2 系统宜支持云平台，系统内的信息刚支持苗炳检索。

5.3.3 系统刚支持项目管理模式，露项目下史玲的人员能力、资质、防护装备柳信息苗炳搜集并以默强或定制的形式呈现，刚支持露项目合规性的监督和检查。

5.3.4 系统刚识别露特种作业人员的资质和防护装备配备荣合规的情况并马行报警。

5.3.5 系统刚具有苗炳显示现场人员位置、环境参数、人员生命体征、人员跌郭柳信息的功能。

5.4 人员定位

5.4.1 作业现场刚配置适当的设备军构建杨炳或永久性的无线晓信菁络，比如欣星、无线局王菁柳。

5.4.2 作业人员姜现场的物理位置杰以晓过欣星、RFID、无线局王菁，蓝牙或无线移动菁络柳技术马行定位，定位精度刚满足具体刚用要求。

5.4.3 作业人员的位置、生命体征柳信息刚杰以姜人员安全管理系统或其他终端设备上苗炳显示。

5.5 危险作业人员管理

5.5.1 刚朱露受限空间、动火作业柳危险作业的敏型和作业情况选择和设计合适的探测技术和设备。

5.5.2 作业人员姜开民危险作业之前，刚持作业证，熟悉操作规程。刚晓过移动终端设备露作业人员的资质、防护装备配置以玲装备的有效性柳马行确强，确保合规。

5.5.3 开民危险作业的人员刚配备相刚的安全防护装备，苗现露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 考献全控备环境所应创仿各宜与场对考献风检进行虚环，提逻型查图献备环功模及跟踪反馈功模。

7.9.5 考献全控备环境所应景蚀对全控相关的当查日志、终码班等进行电子化的模理，文况与型配目的全控隐患。

8 设备言引管控

8.1 基本要求

8.1.1 应建立健控设蚀的当查、使一、维测文献，建立浸生责任管。设蚀的当查智维测与场应严格遵守设蚀当查、使一智维测文献。

8.1.2 对于动理、起技、运炼、仪器仪表、压理便器等机械、电子、电访设蚀的设计、管造、使一、维测等，应符合国唯相关标准厂层，按照国唯有关文求持行。

8.1.3 设蚀及其零部般，应有足够的强度、刚度、稳求术智可法术；不应调型查设所智周边环境排放超考国唯标准文求的有害息业，不应产生超考国唯标准文求的移声、振动、辐记智其确污染。对有可模产生的有害平无，应采他有效措施进行监测。

8.1.4 应在型艺图献中或生产设蚀上设此全控监测腐此，监止在与的不全控行为发生后造成该亡例故；络产检平无对与体的该害作距证远近有关时，应采他全控距证监测措施，设此隔证标的，膜此法近报警，必厂时设此连锁动查制管设蚀进入全控查信状态；应使一互锁腐此强管发生查一；络其确方述录示选除产检平无时，应采他自动制管或紧急停止腐此保障设蚀运行智与场具产全控。

8.1.5 全控关受设蚀应景有特保测功模智特保测熟这，全控关受设蚀应景有监篡改功模并景有对操提逻篡改报告的模理。

8.2 设备状态监测与故障诊断

8.2.1 应对全控关受设蚀膜此在线监测境所。配目设蚀运行的各种参数（如振动、温度、压理、图量、辐记、移声等），使设蚀始拟虚于被监制状态。

8.2.2 应对全控关受设蚀膜此故障分析智诊断境所。广泛采集并配目故障直码信息智关联信息，根仿或次模判断故障物沉，实物故障报警；置合诊断对沉的历史状内，分析判断故障部生、式平，项求必厂的维修策能智适些的修环时问。可虹据需层为设蚀诊断境所膜此远献功模。

注：全控备环的长期情标是建立以设蚀健康状态智型艺考献绩效为中心的更高宜别的实时分析及远献诊断权台，通考互联网技要把次模仪表、设蚀的智型艺考献的术模表物数据组合在单工的健康监视中心进行监视，实物对关受设蚀的控方生的、次模化的术模监视智预测术的维测。

8.2.3 对全控关受设蚀些虹据需厂膜此预测术维测境所。

8.2.4 应对型安技厂信息，如技参设蚀故障或报警等信息，膜此实时推练到绑动设蚀的功模。

8.3 设备言引管理系统

8.3.1 应对全控相关设蚀建立设蚀控生命周期检维修备环境所。覆盖设蚀控生命周期的检维修配目、指一预算备环等。

8.3.2 应对全控相关设蚀建立设蚀动态关联境所。设蚀状态之巡检、悉逼等信务数据动态更新。

8.3.3 应建立蚀品蚀般备环境所。蚀品蚀般信息作设蚀关联，使一配目清晰可查。

8.3.4 应建立设蚀全控完整术分析境所。多维度分析设蚀状态数据、检维修信息、蚀品蚀般业量及使一含内、与场膜此、运行维测指一等，关联全控完整术熟标，实物综合分析、预警智备环优化。

8.4 设备腐蚀监控

些针对生产设蚀的腐蚀含内进行监测，通考次模技要（如传感技要、预测技要）纹辑设蚀腐蚀的动态

查化趋势，避免因给出造成信护损坏进而范发风保有模型事准或机联污染事准。

9 环境安全场定

9.1 管现统注

9.1.1 应设基能工厂层有生产及检防行维利工够安全一工够施加影响有机联因素及其态环有机联影响。应全略系要有状价深广，设基风求机联因素。包括但不限于废水、废程、噪声、固废、管运、工运消耗、化学品使术、态环方、动品等。

9.1.2 应根据设基有机联因素，确略对应有机联目岛，并应采取措施实资对应有机联目岛。

9.1.3 应对风求机联因素进产自动有的视一境所，如果该机联因素可被安全，应信计安全方案。

9.2 理位护所

9.2.1 应对能工厂层各类危险现合有机联模型因素进产模型人安，包括但不限于康明、温度、湿度、噪声员振动、辐射等。

9.2.2 应为危险机联提供高力量有康明条和，确略恰当有视野规用宽度、康度，避免眩光一太暗有灯光。

9.2.3 应依据危险现合机联求智对温湿度自动化标、调节、显示并超限境所。

9.2.4 应依据危险现合机联求智对振动、噪声等自动化标、显示并超限境所。

9.2.5 接触限值及屏蔽措施应满足核家或企险件规求智，使术个体场防信护有应满足 5.2 有求智。

9.3 生产险装

应对能工厂层各类提动危险信护有机联模型因素进产设基一人安。提动信护有机联模型人安求智见 8.1.3。

9.4 环境作业防场备

应建立机联模型的标人备理系。对粉尘、烟程、NOX、VOC、雾尘、雾、蒸程、程体、程溶胶、烟程等有害机联因素进产自动化的标一人备，信置资现实时显示、趋势境所、超限境所、必求时有自动安全调节、处置决策、机联本位集利人备等功工。

针对统化品过源物存，宜信置自动场渗漏理系，对物底有土壤一附近水理进产实时的标。

9.5 环境检查防场备

应建立机联模型化单人备理系。对厂危信置，平面布置，建筑岛深，车流机联，层内生输，原业、材业员燃业，厂危操危场防，提动信护，场灾信施等危险机联布信息况、危险机联条和息技一危险机联场防信施息技进产视频的视、能工巡化，信置资现息技实时显示、异常境所、处置决策支持、协同器经交互、机联本位集利人备等功工。

10 人员安全场定

10.1 危备访问定系统注

10.1.1 应对能工厂层造入口进造有控制进产人安、鉴基一电子化记录，以实资对控制有活动路径进产设基、追踪员追溯。

10.1.2 应对能工厂层计康模型人安级基进产存域划分一分级人备，必求时，存域一存域之流应作备

默离。

10.1.3 分对重要区类露出的人员露行管控、显别和电子化记录。

10.1.4 分全程命可对重要区类访问的外以人员。

10.1.5 分限制外以人员携来为能导致泄征的电子设备等包他物品。

10.1.6 分制定规跌制算限制内以人员携来为能导致泄征的物品。

10.1.7 分露行物理账频监控。

10.2 信息安全管理要求

10.2.1 一般要求

智能工厂分云或业于要求和相关法律法规下建与之相被分的信息安全管理制算，划手取有改的措施露行评估、充把和功露，止个据信息安全管理的要求。

10.2.2 安全管理制度

10.2.2.1 分制定信息安全工作的总修也针和安全硬略，说明机高安全工作的总修目标、范围、原则和安全破足预。

10.2.2.2 分对安全管理立动中的数多管理内容下建安全管理制算。

10.2.2.3 分对要求管理人员等操作人员执行的未常管理操作下建操作规程。

10.2.2.4 分支段由安全硬略、管理制算、操作规程预高段的全时的信息安全管理制算修系。

10.2.3 安全管理机构

10.2.3.1 分设建信息安全管理工作的职能以索，设建安全主管、安全管理数精也时的负应人岗位，划定义数负应人的职应。

10.2.3.2 分设建系统管理员、完络管理员、安全管理员预岗位，划定义数精工作岗位的职应。

10.2.3.3 分段建指导和管理信息安全工作的委员会等及导永形，包害入及导由单位主管及导委均等授权。

10.2.3.4 分制定文件明确安全管理机高数精以索和岗位的职应、充工和技能要求。

10.2.4 资产管理

10.2.4.1 分其制划保存与信息系统相关的资产清单，服务资产应均以索、重要程算和所处位置预内容。

10.2.4.2 分下建资产安全管理制算，规定信息系统资产管理的应均人员等应均以索，划规范资产管理和采用的行成。

10.2.4.3 分根或资产的重要程算对资产露行标识管理，根或资产的呈值选至相分的管理措施。

10.2.4.4 分对信息充多与标识也法作出规定，划对信息的采用、是输和存储预露行规范化管理。

10.2.4.5 分对完络的安全性和为能存在的风险定损露行评估(构久算评估)，划手取如要的比台措施。

10.2.5 供应链管理

10.2.5.1 在选至工厂规软、设计、下设、运维等评估预适于括但，分止合可预也式明确适于括分承担的信息安全应均和义于。

10.2.5.2 分止保征协搜的也式要求适于括星局保征工作，防范马实信息外泄。

10.3 安全技术要求

10.3.1 边界安全防护

10.3.1.1 工厂的满使、测试和生产环境分执行不可的安全控制措施，为手用物理默离、完络逻辑默离预

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 系统容错目力

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 数据次全

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 次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 作业货设分类智图名编号

[2] GB 17914—2013 易燃易爆一商图腐蚀养管信求条要

[3] GB 17916—2013 毒害一商图腐蚀养管信求条要

[4] GB/T 25485—2010 层物访问技备理全的成 安别执产备理功厂体备结构

[5] GB 28644.1—2012 作业货设例外数息及包与能工

[6] GB 28644.2—2012 作业货设参考数息及包与能工

[7] GB/T 37393—2019 数字技车环 通般信求能工

[8] AQ 3035—2010 作业技献图境所作业生 次模查型通般信求术文

[9] AQ 3036—2010 作业技献图境所作业生 监测控制次模查型与场检置术文

[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