ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41260—2022

数字化车间信息安全要求

Security requirements for digital factory

2022-03-09 发布　　2022-10-01 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、缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 4
4　数字化车间信息安全总则 …… 4
4.1　数字化车间信息安全范围 …… 4
4.2　数字化车间信息安全基本要求 …… 5
4.3　数字化车间信息安全分析流程 …… 6
5　数字化车间信息安全管理要求 …… 7
5.1　概述 …… 7
5.2　信息安全管理制度 …… 7
5.3　信息安全管理岗位与职责 …… 7
5.4　人员管理 …… 8
5.5　风险管理 …… 8
5.6　物理访问控制管理 …… 9
5.7　运维安全管理 …… 9
5.8　监视和评审信息安全管理的有效性 …… 9
5.9　保持和改进 …… 10
6　数字化车间信息安全技术要求 …… 10
6.1　概述 …… 10
6.2　区域划分与边界防护 …… 11
6.3　身份鉴别与认证 …… 12
6.4　使用控制 …… 12
6.5　资源控制 …… 13
6.6　数据安全 …… 15
6.7　安全审计 …… 15
附录A（资料性）　数字化车间信息安全常见威胁源 …… 17
附录B（资料性）　典型机械制造行业数字化车间信息安全示例 …… 18
B.1　概述 …… 18
B.2　确定保护对象与目标 …… 19
B.3　风险分析与处置 …… 19
B.4　安全防护需求与安全策略 …… 20
B.5　安全确认与评估 …… 21

B.6 运行与维护 …… 22
附录 C（规范性） 数字化车间信息安全增强要求 …… 23
C.1 概述 …… 23
C.2 区域划分与边界防护 …… 23
C.3 身份鉴别与认证 …… 24
C.4 使用控制 …… 24
C.5 资源控制 …… 25
C.6 数据安全 …… 25
C.7 安全审计 …… 26
参考文献 …… 28

图 1 数字化车间信息安全范围(实线部分) …… 5
图 2 数字化车间信息安全分析流程 …… 7
图 B.1 机械制造行业典型架构 …… 18
图 B.2 典型工程/数字化车间安全架构 …… 19

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、重庆信安网络安全等级测评有限公司、浙江中控技术股份有限公司、国能智深控制技术有限公司、深圳市标利科技开发有限公司、宁波和利时信息安全研究院有限公司、中国科学院沈阳自动化研究所、中国电力工程顾问集团华北电力设计院有限公司、北京市劳动保护科学研究所、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、上海工业自动化仪表研究院有限公司、西门子(中国)有限公司、菲尼克斯(南京)智能制造技术工程有限公司、长沙有色冶金设计研究院有限公司、罗克韦尔自动化(中国)有限公司、快克智能装备股份有限公司。

本文件主要起草人：孟邹清、张亚彬、魏振强、潘东波、裘坤、田雨聪、任军民、徐皑冬、马欣欣、刘盈、靳江红、郭永振、董赢、李佳、张晓进、彭小波、张占峰、王玉敏、赵艳领、郭苗、熊文泽、黄焕袍、牛海明、鄢锋、曾祥吉、戚国强、罗方伟、王荣臻。

引　言

数字化车间较传统生产车间具有数字化、网络化、智能化等特点，互联互通互操作成为数字化车间建设的基本特征。生产车间的边界被扩大，传统信息安全的威胁将会渗透到数字化车间内部，而数字化车间内的各类设备、系统设计之初主要是面向可用性而非安全性，信息安全防护能力普遍低下；数字化车间系统化的特性也导致信息安全产生的影响变得更大，一个局部的影响可能导致整个车间的停运；与此同时，物联网及新兴网络和通信技术等的应用也会把外部威胁直接引入到生产现场，因此数字化车间的建设应充分考虑信息安全的因素。

本文件以数字化车间为对象，充分考虑数字化车间的特点，从管理与技术两个方面提出信息安全要求。

数字化车间信息安全要求

1 范围

本文件规定了数字化车间信息安全总则、管理要求和技术要求等。

本文件适用于针对数字化车间的工程设计、设备生产、系统集成、生产运维、安全评估等信息安全活动。

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 37413—2019 数字化车间 术语和定义

IEC 62443-1-1:2009 工业通信网络 网络和系统安全 第1-1部分：术语、概念和模型(Industrial communication networks—Network and system security—Part 1-1:Terminology, concepts and models)

3 术语和定义、缩略语

3.1 术语和定义

GB/T 37413—2019 和 IEC 62443-1-1:2009 界定的以及下列术语和定义适用于本文件。

3.1.1

数字化车间 digital factory;digital workshop

以生产对象所要求的工艺和设备为基础，以信息技术、自动化、测控技术等为手段，用数据连接车间不同单元，对生产运行过程进行规划、管理、诊断和优化的实施单元。

注：在本文件中，数字化车间仅包括生产规划、生产工艺、生产执行阶段，不包括产品设计、服务和支持等阶段。

[来源：GB/T 37413—2019，2.1]

3.1.2

资产 asset

数字化车间拥有或保管的物理或逻辑对象，该对象对数字化车间具有潜在或实际的价值。

注：在工业自动化和控制系统的情况下，具有最大直接可测量价值的实物资产可能是受控设备。

[来源：IEC 62443-1-1:2009，3.2.6，有修改]

3.1.3

生产系统 production system

为完成数字化车间生产任务而需要的各类硬件、软件以及人员的集合。

注：数字化车间生产系统包括但不限于。

a) 可编程逻辑控制器(PLC)、智能电子设备(IED)、分布式控制系统(DCS)、紧急停车系统(ESD)、安全仪表系统(SIS)、监视控制与数据采集(SCADA)系统、运动控制(MC)系统、数控系统(CNC)、柔性制造系统(FMS)等系统。

b) 相关的信息系统，例如专用设备监视器、图形界面、过程历史记录、制造执行系统(MES)。

3.1.4

感知控制层 the layer of perception and control

定义了感知和操控车间物理流程的活动。

注：典型的运行时限是秒，甚至更快。

[来源：GB/T 20720.3—2010，4.2，有修改]

3.1.5

监控层 the layer of monitoring

定义了监测和控制车间物理流程的活动。

注：典型的运行时限是小时、分钟和几分之几秒。

[来源：GB/T 20720.3—2010，4.2，有修改]

3.1.6

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：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。

[来源：IEC 62443-1-1：2019，3.2.99，有修改]

3.1.7

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安保策略。

[来源：GB/T 30976.1—2014，3.1.1]

3.1.8

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

[来源：GB/T 20984—2007，3.17]

3.1.9

信息安全风险 information security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

[来源：GB/T 20984—2007，3.6]

3.1.10

风险分析 risk analysis

系统地使用信息来识别风险来源和估计风险。

[来源：GB/T 30976.1—2014，3.1.8]

3.1.11

风险处置 risk treatment

选择并且执行措施来更改风险的过程。

[来源:GB/T 30976.1—2014,3.1.11]

3.1.12

安全措施 security measure

为保护资产、抵御威胁、减少脆弱性、降低安全事件的影响而实施的各种实践、规程和机制。

[来源:GB/T 20984—2007,3.15,有修改]

3.1.13

残余风险 residual risk

经过风险处置后遗留的风险。

[来源:GB/T 30976.1—2014,3.1.6]

3.1.14

安全事件 security incident

系统、服务或网络的一种可识别状态的发生,它可能是对安全策略的违反或防护措施的失效,或未预知的不安全状况。

[来源:GB/T 20984—2007,3.14]

3.1.15

可用性 availability

数据或资源的特性,被授权实体按要求能访问和使用数据或资源。

[来源:GB/T 20984—2007,3.3]

3.1.16

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。

注:包括数据完整性和系统完整性。

[来源:GB/T 20984—2007,3.10]

3.1.17

保密性 confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[来源:GB/T 20984—2007,3.5]

3.1.18

区域 zone

共享相同信息安全要求的逻辑资产或物理资产的集合。

注:区域具有清晰的边界。一个信息安全区域的信息安全策略在其内部和边界都要强制执行。

[来源:IEC 62443-3-3:2013,3.1.47]

3.1.19

边界 boundary

软件、硬件或者其他物理屏障,限制进入系统或者部分系统。

[来源:IEC 62443-1-1:2009,3.2.19]

3.1.20

审计 audit

独立审查和记录检查,以确保遵守既定的政策和操作程序,并建议必要的控制变更。

[来源:IEC 62443-1-1:2009,3.2.11,有修改]

3.1.21

访问控制 access control

保护系统资源防止未经授权的访问;系统资源使用的过程是根据安全策略规定的,并且根据该策略

只允许被授权的实体(用户、程序、过程或其他系统)。

[来源:IEC 62443-1-1:2009,3.2.2]

3.1.22

鉴别 authentication

身份所声明特征正确性的保证行为。

注:在一个控制系统中,鉴别是允许访问系统资源的先决条件。

[来源:IEC 62443-3-3:2013,3.1.4]

3.1.23

授权用户 authorized user

依据安全策略可以执行某项操作的用户。

[来源:GB/T 33009.4—2016,3.1.3]

3.2 缩略语

下列缩略语适用于本文件。

APT:高级持续性威胁(Advanced Persistent Threat)

ARP:地址解析协议(Address Resolution Protocol)

CAD:计算机辅助设计(Computer Aided Design)

CAE:计算机辅助工程(Computer Aided Engineering)

CNC:数控系统(Computer Numerical Control)

DCS:分布式控制系统(Distributed Control System)

DDoS:分布式拒绝服务(Distributed Denial of Service)

DMZ:非军事区(Demilitarized Zone)

DNC:分布式数控(Distributed Numerical Control)

DoS:拒绝服务攻击(Denial of Service)

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

ESD:紧急停车系统(Emergency Shutdown Device)

FMS:柔性制造系统(Flexible Manufacturing System)

HMI:人机界面(Human Machine Interface)

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

PLC:可编程逻辑控制器(Programmable Logic Controller)

PLM:产品生命周期管理(Product Lifecycle Management)

RFID:无线射频识别(Radio Frequency Identification)

SIS:安全仪表系统(Safety Instrumented System)

VLAN:虚拟本地网(Virtual Local Area Network)

4 数字化车间信息安全总则

4.1 数字化车间信息安全范围

一个企业/工厂根据不同的功能可以划分为三个层次,如图1所示,分为基础层、执行层、管理层。

数字化车间的基础层包括了数字化车间生产制造所必需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。

这里基础层通常可以细分为两层：感知控制层与监控层。

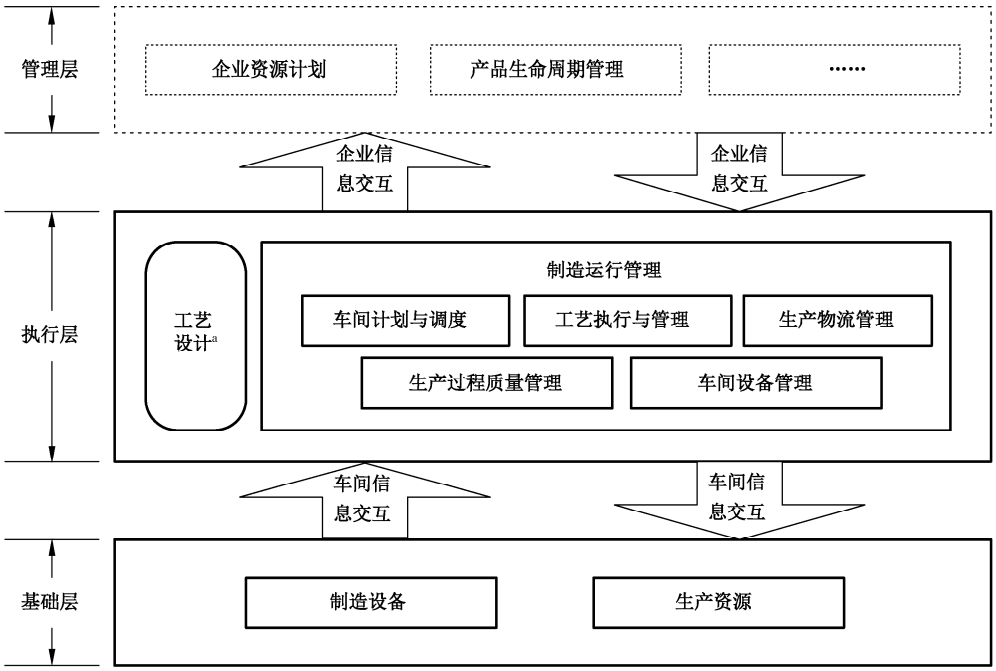
注：这里的设备包含但不限于 DCS、PLC、ESD、SIS、CNC、HMI、工业机器人、各种传感器、执行器、操作面板等。

数字化车间的执行层主要包括车间计划与调度、生产物流管理、工艺执行与管理、生产过程质量管理、车间设备管理五个功能模块，对生产过程中的各类业务、活动或相关资产进行管理，实现车间制造过程的数字化、精益化及透明化。由于数字化工艺是生产执行的重要源头，对于部分中小企业没有独立的产品设计和工艺管理情况，可在数字化车间中建设工艺设计系统，为制造运行管理提供数字化工艺信息。以 MES 系统为代表的面向车间执行层的生产信息化管理系统，该系统会进行数据采集、生产调度、代码下载、参数配置等各项功能的执行。

数字化车间的管理层以 ERP 为代表的企业资源管理，负责企业订单的接收，人力、工资等信息的管理，包括但不限于 PLM、CAD、CAE 等各种资源。

数字化车间以物理车间为基础，物理车间的资产属于数字化车间的一部分，不在物理车间内部但是通过网络等方式连接的设备/系统仍然作为数字化车间的一部分，如 MES 系统使用的服务器可能放置于专门的机房，车间与机房通过光纤方式进行连接通信。

因此，数字化车间信息安全的范围包括基础层和执行层全部与信息安全相关的系统/活动。数字化车间信息安全保护的对象包括数字化车间的物理资产、逻辑资产（如工艺配方等）。



[a] 数字化车间/智能工厂可选功能。

图 1　数字化车间信息安全范围（实线部分）

4.2　数字化车间信息安全基本要求

4.2.1　保障生产安全要求

信息安全措施应有利于增强安全相关系统对内部攻击、外部攻击和误操作的防御。

信息安全措施不应对生产紧急事件处理产生妨碍，或者虽有影响但经过充分评估后可以实施。

4.2.2　保障连续生产要求

信息安全技术措施不应对自动化控制装备的通讯端口、控制网络产生连续或阶段性的网络冲击对

控制实时性和连续性的不利影响应控制在允许范围。

对控制设备和操作站点采取信息安全技术措施前，应充分测试和验证该技术措施是否影响控制设备和工业软件的运行。

4.2.3 不影响控制装备互联互通要求

采取信息安全管理和技术措施前应考虑到事实上多种工业控制协议设备间的互联互通，对于采用私有协议或国际现场总线标准的控制和通讯设备可考虑采取网段隔离等措施，不宜更改相关通讯标准协议。

4.2.4 适用性要求

应考虑数字化车间重要程度，以及系统脆弱性、威胁和安全风险现状，平衡经济性和安全性，结合系统架构和技术情况，采用适宜的安全防护措施/补偿对抗措施。

4.2.5 动态性要求

应考虑数字化车间全生命周期内风险与信息安全需求的变化，及时采取相应措施。

4.2.6 内生安全与纵深防御相结合要求

应结合内生安全技术与多层次纵深防御措施来有效保障信息安全，宜优先采用具备内生安全技术的控制装备，从而抵御相关技术和管理措施失效或过失情况下的风险。

4.2.7 管理和技术相结合要求

数字化车间的信息安全应综合考虑管理和技术措施，技术措施应通过必要的管理措施来保障落实和执行。

4.3 数字化车间信息安全分析流程

如图 2 所示，对于一个数字化车间在建设阶段应充分考虑安全需求，安全需求的前提是基于目标对象的确定，进而进行必要的危险和风险分析之后得出的，对于安全需求要进行评估，进而制定安全策略和安全措施，在数字化车间实际投入运行之前应对安全措施进行评估和确认。

注：对安全措施进行评估和确认可以通过线上测试和分析实现。

当数字化车间进入运行维护阶段，应定期和根据实际需要进行风险评估，根据评估结果通过修改、加强、增加安全措施来应对风险变化导致的安全能力下降，其中安全措施包括管理措施和技术手段。

数字化车间的常见威胁和风险点见附录 A，实际的分析处理过程见附录 B。

数字化车间信息安全能力由管理措施、技术手段各方面因素综合决定，具体要求见第 5 章、第 6 章。

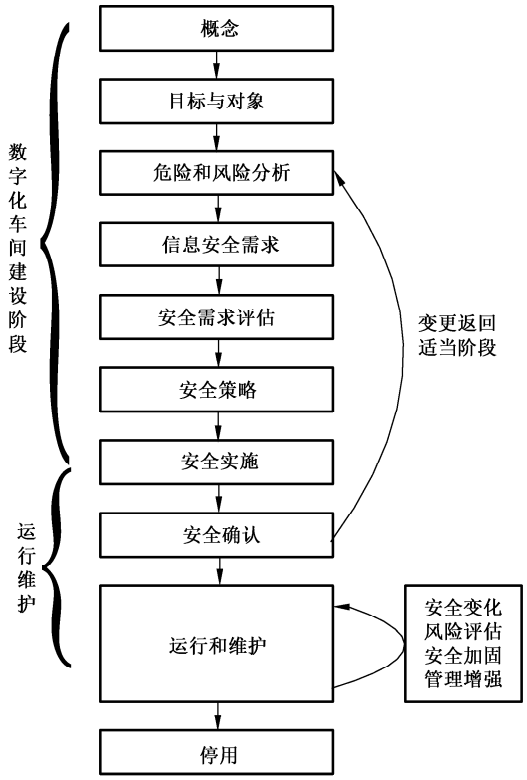


图 2　数字化车间信息安全分析流程

5　数字化车间信息安全管理要求

5.1　概述

数字化车间的拥有者或运营者(以下简称“组织”)应充分识别、分析、评价、管理、监视和评审组织所面临安全风险,建立并维护信息安全管理要求的措施,明确信息安全管理职责,分配和管理资源,运用过程方法实现数字化车间的正常运行,并采取有效的措施评估、分析和改进,以满足数字化车间信息安全管理的要求。

5.2　信息安全管理制度

在数字化车间信息安全管理制度的制定中应:

a)　按照信息安全管理方针和策略,制定数字化车间的信息安全工作原则与目标;

b)　对数字化车间的安全管理活动建立相应的信息安全管理制度;

c)　对管理人员和操作人员执行的日常信息安全管理操作建立操作规程或者作业指导书;

d)　通过正式、有效的方式发布,并进行版本控制。

5.3　信息安全管理岗位与职责

应通过清晰的岗位设置、明确的信息安全职责划分,支持数字化车间的信息安全管理。

a)　设立数字化车间的信息安全管理岗位,并明确定义岗位职责。

b)　各岗位应配备相应的管理人员,并应明确定义各级人员的职责。

c)　关键岗位应配备多人共同管理。

d)　信息安全管理的角色和职责应落实到具体的责任人、管理者、具体的工位、具体的单元操作等。

5.4 人员管理

5.4.1 人员录用与离职管理

在数字化车间的人员录用与离职管理中应：

a) 对被录用关键岗位信息安全管理人员的身份背景、资质等进行审查；

b) 及时终止离职信息安全管理人员的所有访问权限，更换相应访问密码，收回所授予的各种身份证件、钥匙以及组织提供的软硬件设备等。

5.4.2 人员培训、意识和能力

应通过以下方式，确保所有被赋予信息安全管理职责的人员具有执行所要求任务的能力：

a) 确定从事数字化车间信息安全管理工作的人员所必要的能力；

b) 对各类人员进行信息安全意识教育和岗位技能培训，或采取其他措施（如聘用有能力的人员）以满足这些能力需求；并告知相关的安全责任和惩戒措施；

c) 对关键岗位的人员进行信息安全技能考核；

d) 评价所采取措施的有效性；

e) 保存教育、培训、技能、经历和资格的记录。

5.4.3 外部人员访问管理

在数字化车间的外部人员访问管理中应：

a) 确保外部人员在进入物理访问受控区域前提出书面申请，批准后由专人全程陪同，并登记备案；

b) 确保在外部人员接入网络访问系统前提出书面申请，批准后由专人开设账号、分配权限，并登记备案；

c) 在外部人员离场后及时清除其所有的访问权限。

5.5 风险管理

5.5.1 确定风险管理目标

对数字化车间的风险管理控制目标和控制措施应加以选择和实施，以满足风险评估和风险处置过程中所识别的要求。这种选择应考虑接受风险的准则以及法律法规的要求。

组织宜获得管理者对残余风险的批准。

5.5.2 识别、分析和评价安全风险

应建立、维护数字化车间信息安全风险的识别、评估、分析、评价、处置及控制的方法，并定期实施风险评估：

a) 确定风险评估方法、制定接受风险的准则和识别可接受的风险级别；

b) 定期识别各类风险，如通过连网设备识别风险时应有相应流程或资产面临的危险和可能被威胁利用的脆弱性等；

c) 定期分析和评价各类风险，包括评价安全失效可能对组织造成的影响等；

d) 确定可选措施以消除风险或避免风险等；

e) 在组织的方针策略和可接受风险的准则条件下，主动、客观地接受风险。

5.5.3 风险处置

在数字化车间的风险处置中应：

a) 为管理数字化车间信息安全风险制定处置计划，该计划应包含适当的管理措施、资源、职责和优先顺序等；
b) 实施风险处置计划达到已识别的控制目标，包括资金安排、角色和职责的分配；
c) 实施所选择的控制措施满足控制目标；
d) 确定如何测量所选择的控制措施或控制措施实际的有效性，并指明如何运用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果；
e) 管理数字化车间信息安全相关的资源；
f) 实施能够迅速检测安全事件和响应安全事件的规程和其他控制措施。

5.6 物理访问控制管理

物理访问控制基本要求应包括但不限于：

a) 对数字化车间出入口进出的人员进行控制、鉴别和记录；
b) 对数字化车间划分区域进行管理，必要时，区域和区域之间应物理隔离；
c) 全程陪同对受控区域访问的外部人员；
d) 限制外部人员携带可能导致泄密的电子设备或其他物品如手机、相机、电子记录仪等；
e) 制定规章制度限制内部人员携带可能导致泄密的物品；
f) 对重要区域进行视频监控。

5.7 运维安全管理

在数字化车间的运维安全管理中应：

a) 制定并发布数字化车间安全运维规程，定期对安全运维规程进行评审和更新；
b) 根据厂商或供应商的规格说明以及组织的要求，对数字化车间设备和系统的运维进行规划、实施、记录，并对维护和修理记录进行评审；
c) 审批和监视所有运维行为，不论被维护对象是在现场还是被转移到其他位置；
d) 在对系统或组件维护或修理后，检查所有可能受影响的安全控制措施以确认其仍能正常发挥功能；
e) 数字化车间设备或系统的第三方运维商承诺未经用户同意不得采集用户相关信息、不得远程控制用户设备或系统；
f) 如果采用远程运维的方式，组织根据产品的运维需求，为远程控制端口设置控制权限和控制时间窗；在远程维护完成后，组织安排专人立即关闭为远程维护需求开放的权限设置；
g) 完整地记录所有运维的工作计划、要求、过程和完成情况，并存档；
h) 能够对所有运维操作记录进行安全审计，审计记录应定期备份，避免受到未预期的删除、修改或覆盖等；
i) 定期开展风险评估，对识别和发现的安全漏洞和隐患及时进行修补。

5.8 监视和评审信息安全管理的有效性

在监视和评审数字化车间信息安全管理的有效性时应：

a) 执行监视评审规程和其他控制措施：

- 迅速检测过程运行结果中的错误；
- 迅速识别即将发生的和已发生的安全违规和事件；
- 帮助管理者确定分配给人员的安全活动或通过信息技术实施的安全活动是否按期望执行；
- 帮助检测并预防安全事件；
- 确定安全违规的解决措施是否有效。

b) 在考虑安全事件、有效性测量结果、所有相关方的建议和反馈的基础上，进行信息安全管理有效性的定期评审(包括满足信息安全管理方针和目标，以及安全控制措施的评审)；

c) 测量控制措施的有效性以验证安全要求是否被满足；

d) 按照计划时间间隔进行风险评估的评审，以及对残余风险和已确定的可接受风险及级别进行评审，应考虑以下方面的变化：

- 组织；
- 数字化车间升级或更新；
- 业务目标和过程；
- 已识别的威胁；
- 已实施的控制措施的有效性；
- 外部事态，如法律法规环境的变更、合同义务的变更和社会环境的变更。

e) 考虑监视评审活动的结果，以更新安全计划；

f) 记录可能影响数字化车间信息安全的有效性或执行情况的措施和事态。

5.9 保持和改进

在保持和改进数字化车间信息安全管理时应：

a) 实施易识别的信息安全管理改进措施；

b) 采取纠正和预防措施，从其他组织和组织自身的安全经验中吸取教训；

c) 向所有相关方沟通纠正和预防措施、改进情况，其详细程度与环境相适应，需要时商定如何进行；

d) 确保改进达到了预期目标。

6 数字化车间信息安全技术要求

6.1 概述

6.1.1 安全要素

本文件以区域划分与边界防护、身份鉴别与认证、使用控制、资源控制、数据安全与安全审计作为数字化车间信息安全技术要求的基本要素，具体为：

a) 区域划分与边界防护

应从企业和数字化车间系统整体角度来考虑信息安全，通过区域划分和边界防护来实现纵深防御，保障数字化车间生产系统受到攻击时不扩散到另外的区域。

b) 身份鉴别与认证

应防止未经授权的访问，如用户名与密码形式的身份鉴别与认证。

c) 使用控制

应防止未经授权的使用，即使用户、软件等实体通过了鉴别，不同授权用户、软件等实体对数字化车间生产系统的操作与使用不得超过其所分配的权限。

d) 资源控制

应控制资源的使用防止因非法或超限使用资源从而影响生产系统的可用性、生产连续性等。

e) 数据安全

应保证静态数据和通信数据的可用性、完整性、保密性。

f) 安全审计

应对生产系统的日志、状态、报警等信息进行核查来检测系统是否处于预期的安全设置。

6.1.2 安全要求说明

本文件中规定的安全要求是实现数字化车间信息安全能力的基本要求。如果需要更高的要求，应符合附录C的规定。

6.2 区域划分与边界防护

6.2.1 感知控制层基本要求

在数字化车间感知控制层对区域划分与边界防护的基本要求为：

a) 感知控制层宜和对应的监控层划分为同一区域；

b) 如有必要感知控制层内宜可划分多个子区域；

c) 如有必要在感知控制层和对应监控层之间可设置边界，运用安全审计等非阻断型策略；

d) 与感知控制层相连的其他所有网络或系统，如没有在同一安全区域，则与感知控制层相连的边界应满足边界防护的基本要求；

e) 如有物联网或其他无线网络与感知控制层有线网络相连，物联网或其他无线网络应作为各自独立的区域，在与感知控制层有线网络之间设置边界防护；

f) 如感知控制层直接与云相连，应按照纵深防御的原则整体进行边界防护。对于设备直接上云的情况应优先配置设备的边界防护，如果设备的边界防护能力不足，应在云端做虚拟边界防护。

6.2.2 监控层基本要求

在数字化车间监控层对区域划分与边界防护的基本要求为：

a) 监控层宜和对应的感知控制层划分为同一区域，此区域在与其他区域相连时应做好边界防护；

b) 如有必要监控层内宜可划分多个子区域；

c) 与监控层相连的其他所有网络或系统，如没有在同一安全区域，则与监控层相连的边界应满足边界防护的基本要求；

d) 监控层和执行层可为不同区域，在监控层与执行层之间应满足边界防护基本要求；应部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-mail、Web、Telnet、Rlogin、FTP等通用网络服务；

e) 如有物联网或其他无线网络与监控层有线网络相连，物联网或其他无线网络应作为各自独立的区域，在与监控层有线网络之间设置边界防护；

f) 如监控层直接与云相连，应按照纵深防御的原则整体进行边界防护。对于边缘终端直接上云的情况应优先配置边缘终端的边界防护，如果边缘终端的边界防护能力不足，应在云端做虚拟边界防护。

6.2.3 执行层基本要求

在数字化车间执行层对区域划分与边界防护的基本要求为：

a) 执行层应整体作为一个区域；
b) 执行层与管理层可为不同区域，在执行层和管理层之间应满足边界防护基本要求；可设置网络隔离设备，禁止管理层未经协议转换直接访问执行层；
c) 如有物联网或其他无线网络与执行层相连，物联网或其他无线网络应作为各自独立的区域，在与执行层之间设置边界防护；
d) 如执行层直接与云相连，应按照纵深防御的原则整体进行边界防护，同时云端应做必要的虚拟边界防护。

6.3 身份鉴别与认证

6.3.1 感知控制层基本要求

在数字化车间感知控制层对身份鉴别与认证的基本要求为：
a) 应保证登录、操作与维护系统人员为可信人员，防止出现非相关人员的访问，影响设备或系统安全运行；
b) 系统应保证外部登录的设备为可信设备，禁止任何不可信设备的接入；
c) 系统内部设备连接外部网络时，应经过上网认证；
d) 系统应具备记录连接事件的功能，以保证所有的连接均可查询；
e) 如果该层使用了远程访问，系统应具备对远程访问设备身份鉴别的能力。

6.3.2 监控层基本要求

在数字化车间监控层对身份鉴别与认证的基本要求为：
a) 应保证登录、操作与维护系统人员为可信人员，防止出现非相关人员的访问，影响设备或系统安全运行；
b) 系统应提供访问用户身份鉴别和认证的能力；
c) 对于使用口令鉴别机制的生产系统，口令应具有一定的复杂性，且需在多次尝试密码失败后，延长重新输入密码等待时间；
d) 系统内部设备连接外部网络时，应经过上网认证；
e) 系统应具备访问记录与事件记录功能；
f) 如果使用了无线网络，无线系统应具备识别接入设备并阻止未经授权设备接入的能力。

6.3.3 执行层基本要求

在数字化车间执行层对身份鉴别与认证的基本要求为：
a) 系统应具备对操作人员身份鉴别的能力；
b) 使用口令鉴别机制的系统，口令应具有一定的复杂性；
c) 系统应具备访问记录与事件记录功能。

6.4 使用控制

6.4.1 感知控制层基本要求

在数字化车间感知控制层对使用控制的基本要求为：
a) 数字化车间各区域间应具有相互访问控制的能力，保证不同区域之间存在隔离，如通过VLAN、路由、防火墙等方式；
b) 系统应具备可配置的使用限制能力，对内部所有可能会被外部接入的接口进行接入限制管理，

如现场交换机的网口，现场工控机的 USB 口、网口等，以防止非授权设备的接入；

c) 系统应具备限制非必要通讯端口、协议和服务的能力；

d) 系统应具备限制不同区域操作或维护人员访问权限的能力；

e) 系统同一区域应实现对不同操作或维护人员实行不同控制权限的能力；

f) 如果使用了无线网络，无线系统应具备识别接入设备并阻止未经授权设备接入的能力；

g) 如果使用了无线网络，工厂应保证使用的无线信道在此无线覆盖区域未曾被占用。

6.4.2 监控层基本要求

在数字化车间监控层对使用控制的基本要求为：

a) 系统应具备可配置的使用限制能力，防止非授权设备的接入；

b) 系统应具有为不同授权用户提供不同权限的能力，以支持职责分离和最小权限；

c) 系统应提供对第三方未经兼容性测试的可能造成生产系统损害的应用程序或移动代码执行使用限制的能力；

d) 应及时为数字化车间采取补丁升级措施，在安装前应对补丁进行严格的安全评估和测试验证；

e) 数字化车间的远程访问端口应具有访问控制措施，对从发起方的访问进行源地址、目的地址、源端口、目的端口和协议等项目的控制。

6.5 资源控制

6.5.1 感知控制层基本要求

在数字化车间感知控制层对资源控制的基本要求为：

a) 应通过设定设备接入方式、网络地址范围等条件限制设备接入该层网络；

b) 网络化的感知控制设备应提供能力：在 DoS 事件时能切换到降级模式下继续运行；

c) 应能够监视接入该层网络的感知控制设备的网络负荷、流量、连接数、会话数等网络资源信息；应支持根据安全策略要求对感知控制设备端允许通过的数据流量、支持的连接数、会话数进行限制；

d) 应能够监视接入该层网络的感知控制设备及相关网络设备的运行状态，例如设备的 CPU 负荷、内存使用情况、设备故障报警信息等；

e) 感知控制设备应对存储于内存中的配置信息、控制程序、数据进行监控，在系统运行时应限制对感知控制设备的关键数据（包括控制程序代码、组态配置信息等）的访问；

f) 网络化的感知控制设备或网络设备应提供能力：限制信息安全功能的资源使用，以防止资源耗尽；

g) 网络化的感知控制设备或网络设备应在不影响正常设备使用的前提下，提供关键文件的识别和定位，以及用户级和系统级的信息备份（包括系统状态信息）的能力，且能验证备份机制的可靠性；

h) 网络化的感知控制设备或网络设备在受到破坏或发生失效后，应提供能力：恢复和重构设备到一个已知的安全状态；

i) 网络化的感知控制设备或网络设备应提供应急电源切换能力，切换不影响设备的运行状态；

j) 网络化的感知控制设备或网络设备应提供禁用无用功能、端口、协议和服务的能力；

k) 该层网络应能识别并支持指示所有连接的设备。

6.5.2 监控层基本要求

在数字化车间监控层对资源控制的基本要求为：

a) 应通过设定终端接入方式、网络地址范围等条件限制终端及设备接入该层网络；
b) 应支持根据安全策略设置登录终端的操作超时锁定；
c) 该层边界处应提供检测 DoS 事件的能力；
d) 该层边界处应支持根据安全策略要求对允许访问主机、服务器和感知控制设备端的协议、端口、数据流量、支持的连接数、会话数等进行限制；
e) 接入监控层的感知控制设备应提供能力：在 DoS 事件时能切换到降级模式下继续运行；
f) 应能够监视接入该层网络的主机、服务器和感知控制设备的网络负荷、流量、连接数、会话数、会话响应时间等网络资源信息；
g) 应能够监视接入该层网络的主机、服务器、软件程序、感知控制设备及相关网络设备的运行状态，例如设备的 CPU 负荷、内存使用情况、设备故障报警信息等；
h) 应提供能力限制主机、服务器、软件程序、网络设备对感知控制设备的关键数据（包括控制程序代码、组态配置信息等）的访问；
i) 主机、服务器、软件程序、网络设备应提供能力：限制信息安全功能的资源使用，以防止资源耗尽；
j) 主机、服务器、软件程序、网络设备应在不影响正常使用的前提下，提供关键文件的识别和定位，以及用户级和系统级的信息备份（包括系统状态信息）的能力，且能验证备份机制的可靠性；
k) 应对关键主机、服务器、网络设备提供应急电源切换能力，切换不影响主机、服务器、网络设备等的运行状态；
l) 主机、服务器、网络设备应提供禁用无用功能、端口、协议和服务的能力；
m) 该层网络应能识别并支持指示所有连接的主机、服务器、设备；
n) 通过 HMI 接口应能获取并指示所有网络化的感知控制设备、主机、服务器、网络设备及其特性、运行状态、故障信息。

6.5.3 执行层基本要求

在数字化车间执行层对资源控制的基本要求为：

a) 应通过设定终端接入方式、网络地址范围等条件限制终端及设备接入该层网络；
b) 应支持根据安全策略设置登录终端的操作超时锁定；
c) 该层边界处应提供检测 DoS 事件的能力；
d) 该层边界处应支持根据安全策略要求对允许访问主机、服务器端的协议、端口、数据流量、支持的连接数、会话数等进行限制；
e) 应提供能力限制主机、服务器、软件程序、网络设备对感知控制设备的关键数据（包括控制程序代码、组态配置信息等）的访问；
f) 主机、服务器、软件程序、网络设备应在不影响正常使用的前提下，提供关键文件的识别和定位，以及用户级和系统级的信息备份（包括系统状态信息）的能力，且能验证备份机制的可靠性；
g) 应对关键主机、服务器、网络设备提供应急电源切换能力，切换不影响主机、服务器、网络设备等的运行状态；
h) 主机、服务器、网络设备应提供禁用无用功能、端口、协议和服务的能力；
i) 该层网络应能识别并支持指示所有连接的主机、服务器、设备；
j) 通过 HMI 接口应能获取并指示所有网络化的感知控制设备、主机、服务器、网络设备及其特

性、运行状态、故障信息。

6.6 数据安全

6.6.1 感知控制层基本要求

连接在系统中的感知控制层设备应满足系统对数据安全的可用性、完整性和保密性的基本要求，包括：

a) 应提供多层的独立防护，来确保数据的安全性，从而保障系统安全；
b) 应通过物理访问保护机制，如控制器的访问等级功能、防护门的钥匙锁、带读卡器和 PIN 的防护门、视频监控等；
c) 应通过硬件的信息安全解决方案：如控制器的防拷贝功能、程序保护技术、网络分段的防火墙保护、带失效关闭的防火墙等；
d) 应通过流程和指令实现数据安全，如对员工的安全培训教育、设置 U 盘访问的白名单规则、关键动作的双重批准等；
e) 应通过安全服务保障生产设备的数据安全，如对系统进行备份和恢复、安全的在线验证等；
f) 可通过安全通信机制。

6.6.2 监控层基本要求

连接在系统中的监控层应满足系统对数据安全的可用性、完整性和保密性的基本要求，包括：

a) 应通过隔离区 DMZ 进行数据交换以加强防护效果，避免直接访问自动化网络；
b) 通过互联网或者移动网络进行远程访问时应进行保护，防止工业间谍活动和蓄谋的破坏；可通过对数据传输进行加密，并通过安全模块或者互联网和移动无线路由器进行访问控制；
c) 可通过环网增强网络的可用性。

6.6.3 执行层基本要求

连接在系统中的执行层应满足系统对数据安全的可用性、完整性和保密性的基本要求，包括：

a) 连接在执行层中的设备应保证其操作系统、软件和硬件具备对应的安全性和健壮性，以抵御恶意软件的攻击或者人为破坏的造成的影响；
b) 应通过设备和系统构建信息安全网络构架；
c) 应通过信息安全网络构建抵御非授权访问的风险，实现访问保护和加密的数据交换等。

6.7 安全审计

6.7.1 感知控制层基本要求

关键生产系统中的重要软/硬件设备应具备日志存储和防篡改的功能。

6.7.2 监控层基本要求

在数字化车间监控层对安全审计的基本要求为：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、主体标识、客体标识、事件是否成功以及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

注 1：安全审计可以是外部审计，也可以是内部审计。

注 2：安全审计需要一定的周期，也可以根据情况随时审计（如出现设备故障高发、产能下降等现象时）。

6.7.3 执行层基本要求

在数字化车间执行层对安全审计的基本要求为：

a） 应在网络边界、重要网络节点、重要应用和数据进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b） 审计记录应包括事件的日期和时间、用户、事件类型、主体标识、客体标识、事件是否成功以及其他与审计相关的信息；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

附 录 A
（资料性）
数字化车间信息安全常见威胁源

数字化车间的信息安全危险既可能来自于数字化车间（数字化车间应有明确的边界）外部，也可能来自于数字化车间内部。威胁来源归结但不限于以下几类：

a） 数字化车间互联互通，上层系统受到的威胁可能渗透到数字化车间内；

b） 数字化车间系统支持的远程维护以及不规范的无线接入点；

c） 数字化车间内设备访问因特网或物联网连接；

d） 移动媒体的不规范使用，USB 设备、光盘、移动硬盘等；

e） 恶意攻击如 DoS、DDoS、APT、人员恶意操作等；

f） 人员误操作。

附 录 B
（资料性）
典型机械制造行业数字化车间信息安全示例

B.1 概述

随着网络技术的快速发展，通过网络来进行生产、管理成为制造业的趋势，利用 DNC 技术进行加工过程管控，已经成为各制造企业的主流选择。DNC 不同于单台机床与计算机的一对一连接，而是多台机床组成网络，编程人员在自己的计算机编制好加工程序（NC 程序）后，通过网络传输到 DNC 系统中，再由 DNC 系统传输到数控机床中或通过数控机床访问 DNC 系统下载程序。

目前部分单位已经实现了以 DNC 系统为中心的生产工控系统网络，通过 DNC 系统进行 NC 程序的下载和上传，实现生产的自动化控制；同时通过 CNC 的采集系统对机床的实时状态进行采集，将采集数据上传至 DNC 服务器，实现设备状态的实时采集和汇总。这些变化大大提高了生产力，但同时也让控制系统面临新的风险与挑战。如图 B.1 所示。

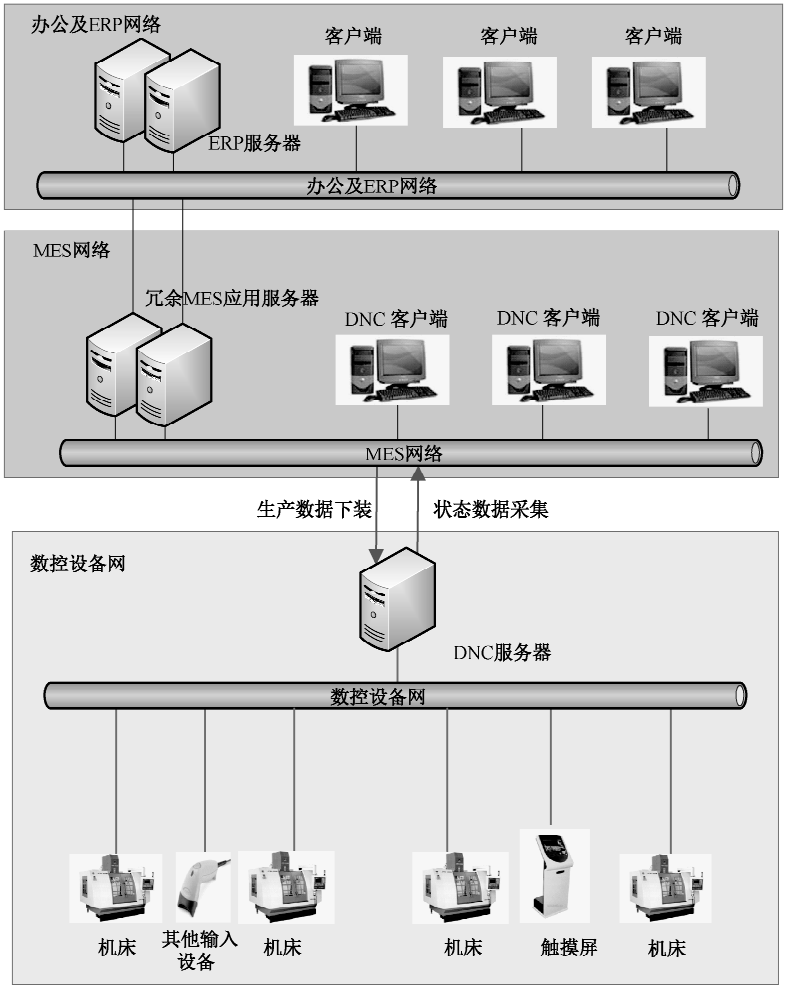


图 B.1 机械制造行业典型架构

根据安全防护需求分析，典型工程/数字化车间安全架构如图 B.2 所示。

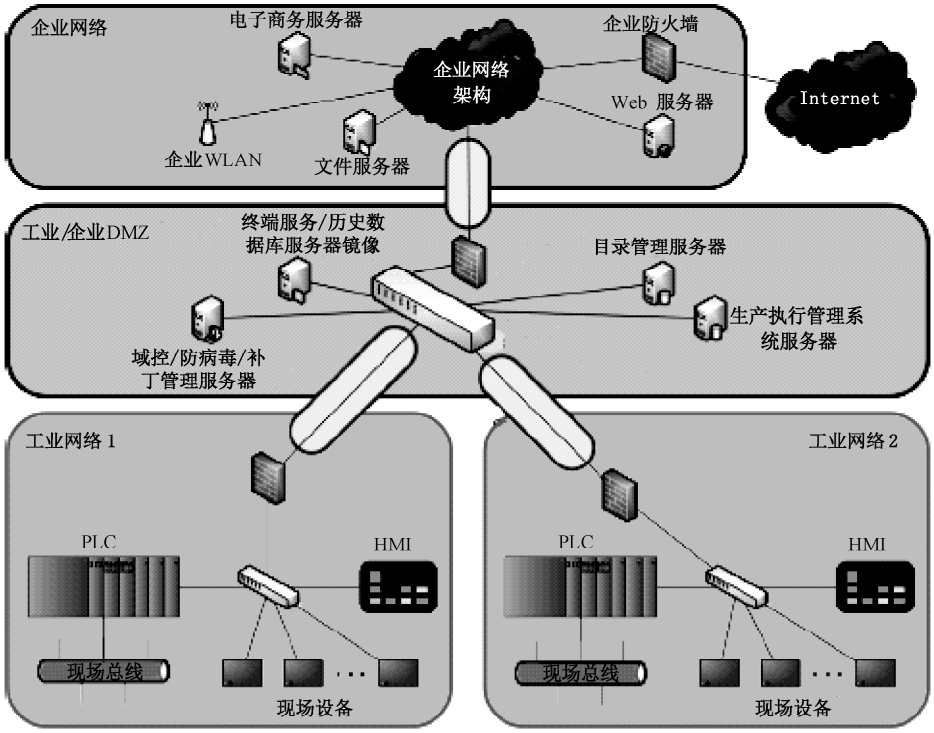


图 B.2　典型工程/数字化车间安全架构

B.2　确定保护对象与目标

对车间进行现场调研，通过对现场相关的网络、设备、数据和应用等资产进行识别与分类，确定各类资产的可用性、完整性和保密性安全属性，然后利用确定的算法将信息资产三个因素的价值综合考虑，确定资产价值大小，从而最终确定要保护的关键资产如下：

a）　网络及网络设备；

b）　现场控制层设备：数控机床；

c）　计算机设备：服务器、工作站、DNC 客户端等；

d）　软件：工业控制系统专有协议、DNC 相关软件、源代码；

e）　数据：工艺配方、数据库数据。

B.3　风险分析与处置

B.3.1　威胁识别

对车间的威胁识别包括：

a）　车间管理网络与控制网络互联互通，上层管理网络受到的威胁与攻击可能渗透扩展到控制网络；

b）　车间不同控制单元间没有进行网络划分与隔离，局部感染可能会影响到全局；

c）　车间控制系统远程维护缺少有效管控手段，可能会造成生产数据的信息泄密或者破坏；

d）　USB 设备、移动硬盘等使用无有效管控手段；

e）　车间工控设备、主机可能遭受恶意代码及病毒攻击，未对操作站主机或者工控设备进行必要的安全配置，一旦能接触访问到被攻击的成功机会很大；

f）　对关键生产工艺数据、工艺配方进行窃取或破坏。

B.3.2 脆弱性识别

对车间的脆弱性识别包括：

a) 工控设备因自身安全性设计方面存在不足，导致其具有可自主修改权限低、安全性差；
b) 数字化车间设备所使用的网络协议及应用软件存在漏洞等；
c) 数字化车间网络系统设计、配置存在缺陷；
d) 网络设备和网络交换设备的链路层安全策略配置不全，通过网络进行恶意攻击如 MAC 洪泛攻击、ARP 攻击、生成树攻击等成功机会很大。

B.3.3 安全风险处置

基于威胁和脆弱性识别以及威胁利用脆弱性导致安全事件发生的可能性分析，并对当前已有安全措施确认后，综合考虑风险控制成本与风险造成的影响，确定需要处置的安全风险如下：

a) 从纵向上来看，控制网络可能会遭受来自办公管理网络的蠕虫、病毒扩散及其他攻击；
b) 从横向上来看，一旦一个控制室单元中感染蠕虫、病毒，就可能向其他的控制区进行扩散，造成全面风险威胁；
c) 攻击者可轻易的将攻击机接入到网络的某一端口，获得与工控设备进行通讯的权限，实施攻击行为；
d) 主机设备对于合法进程无识别，对于病毒无防护，主机较容易感染病毒或启动非法进程，比较容易遭受恶意代码的攻击；
e) 工控设备有的依然采用默认口令或者弱口令；
f) 整个系统网络没有形成统一有效的安全监控及审计体系，网络中如果发生异常通讯或故障，无法及时识别并定位安全问题的源头。

B.4 安全防护需求与安全策略

B.4.1 安全防护需求

基于安全风险处置要求，结合业务现状，安全需求主要体现在以下几个方面：

a) 对车间网络进行安全域划分并对安全域之间实行边界防护，禁止没有防护的控制网络与互联网连接，安全域之间通过防火墙等安全设备进行逻辑隔离；
b) 在工控设备自身安全方面，其可自主修改权限低、安全性差，可被配置程度低，需要实现对设备的安全使用和管理控制，降低自身威胁和整体风险性；
c) 在工业控制网络平台安全方面，如何保证指令在工控系统中传输时不被篡改、丢弃，提供良好的网络平台，提升网络质量，是能正常、正确生产的前提条件；
d) 在工控系统安全方面，如何保证系统不被病毒、木马等恶意程序侵害，如何保证系统不被非授权使用、破坏等，如何保证数据被正确下载和上传，是应解决的安全问题；
e) 在工控应用方面，如何保证系统的权限及使用过程合法、合理，行为可追踪，访问内容可控；
f) 在协议安全方面，应处理好工控设备与现代信息设备协议转换和过程中数据传输的验证等；
g) 在接入安全方面，解决工控网络和工控设备的接入认证问题，防止非法接入；
h) 从设备本身的安全角度看，由于设备的内部结构比较复杂、外部通用接口较多、内部专有接口较多、控制难度较大、系统漏洞很难修补，需加强技术手段进行访问控制和审计；
i) 从设备工作环境看，由于大部分设备安放在比较开放的环境下，接触人员包括公司员工、产品厂商/供应商、协作配套等多类人群，对人员的识别应采取有效的机制，达到有效的控制信息的知悉范围；

j) 从数据管理角度看，由于现场操作人员过多的参与到数据存储、删除等处理活动中，数据存储在本地未进行加密处理，同时又无相关的审计、访问控制措施，尤其在试验环境下，信息泄露问题严重，而目前无论从管理手段还是从技术手段均不能完全满足现有的管理的要求。

B.4.2 安全策略

B.4.2.1 管理措施

指定专人负责车间安全管理，重要数据、工艺配方、文件资料做到专人管理并签署保密协议，使用要有授权并有记录；外部人员的访问与网络接入要有严格的审批与权限控制。

B.4.2.2 技术措施

a) 区域划分与网络防护

1) 区域划分，将具备相同功能和安全要求的设备划分在同一区域内，对网络结构进行重新设计规划，不同的区域划分不同的子网，并按照方便管理和控制的原则为各子网、网段分配地址段。

2) 在区域网络边界部署网络安全隔离设备，分别管控流经网络边界的数据流，安全策略配置数据单向通讯和端口级网络防护策略，保证通讯的可靠性和传输方向的一致性。

3) 每个数控机床和数控设备网之间部署工业防火墙，实现网络区域隔离和通讯管控，工业防火墙具备工业环境适用性和 OPC、ModBus 等工业通讯协议的应用层安全防护功能，可以针对协议本身进行数据合法性检查，保证数据通讯的可控性与可信度。同时工业防火墙还具备链路层数据帧检查功能和 ARP 攻击防护能力，可有效识别通讯设备 IP 和 MAC 是否合法，防止广播风暴和洪泛攻击等对工控网络的威胁。

4) 在网络交换机等设备配置最小化的应用安全策略，根据业务应用需求划分 VLAN、关闭空闲端口，绑定端口接入主机信息（MAC、IP 等），避免设备非法接入以及保证网络接入的安全性。

5) 在网络中部署入侵检测系统，采取旁路监听模式，这样既可以侦测网络中是否存在入侵行为或异常通讯行为，如有异常情况则及时发送安全审计报警日志，又同时保证了工控网络生产数据的正常传递不受影响。

b) 身份鉴别与认证

核查车间网络中网络设备、工控系统等默认口令或弱口令，进行整改并定期更新。

c) 使用控制

1) 在 DNC 系统中的计算机上采用基于可信计算技术的主机安全防护产品为工控系统主机提供白名单方式的软件系统进程管控，进而实现对恶意代码的防范，及时阻止或发现可疑进程的启动，进而为工控系统的主机构建可信的进程运行环境。

2) 计算机上部署基于可信计算技术的移动存储介质的管控及审计系统，实现主机对移动存储介质的身份认证与准入控制，管控移动设备的使用。

3) 重要计算机上安装访问控制终端软件，实现不同授权用户对于主机系统中的程序和文件的使用权限的访问控制及记录。

d) 安全审计

在车间网络部署工控安全审计与异常监测平台，对所有通信进行实时分析、记录、匹配、告警，及时发现各种违规行为以及病毒和黑客的攻击行为，并可对过去发生的网络通信行为进行追溯。

B.5 安全确认与评估

根据实施的安全策略，确定验证和证实系统安全性的目标并制定详细的安全测试计划，定义测试所

采取的步骤，用测试、分析、观察和演示的方法验证和证实系统安全需求。

对系统安全性进行检测或证实，使用渗透测试工具、工控协议漏洞检测设备、网络分析系统等工具设备通过网络对工控系统与设备进行攻击与网络信息收集；使用病毒样本、非法 U 盘等对主机系统与设备进行破坏，实际记录测试结果，出具测试报告。

对检测结果与检测报告进行分析，通过与安全需求对照，确定系统的安全性满足车间的安全需求，安全策略得到正确有效的实施。

B.6 运行与维护

信息安全是一个长期持久的工作，车间的信息安全解决方案实施投入运行后，需要建立一个长效的安全运行机制，才能使车间的信息安全进入持续改进的良性循环。进入运行维护阶段后须重点关注：运行管理和控制、变更管理和控制、安全状态监控、安全自查和持续改进等。措施如下。

a) 制定车间安全运维相关制度规程。明确安全运维具体责任人，建立详细的维护操作流程与相关表单。

b) 明确现场运维和远程运维的管理要求，对运维账号的申请与管理、运维行为的规范等提出具体要求，对现场运维尤其是远程运维进行严格审批和监视。

c) 在车间网络部署安全运维统一管理平台，自动采集车间所有安全设备、主机服务器、网络通信、应用等的运行状态和审计日志等数据，并利用大数据、数据挖掘等先进技术分析网络行为及用户行为等因素所构成的网络态势。为用户提供安全动态监控运维平台，对当前网络及设备安全状态进行集中、实时监控，发现异常及时告警，提醒用户及时处理。

d) 运行过程中须及时了解和控制运行过程中的安全风险，应定期进行风险评估，评估内容包括对车间保护对象的威胁、脆弱性等方面，并出具风险评估报告。

e) 当车间的业务流程、系统状况发生重大变更时，如“增加新的应用或应用发生较大变更、网络结构和连接状况发生较大变更、技术平台大规模的更新、系统扩容或改造、发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件”，也须进行风险评估。

附 录 C
（规范性）
数字化车间信息安全增强要求

C.1 概述

用户在实现数字化车间信息安全技术基本要求的同时，可以根据实际需要采用本附录的增强要求以提高数字化车间的信息安全能力。

C.2 区域划分与边界防护

C.2.1 感知控制层增强要求

在数字化车间感知控制层对区域划分与边界防护的增强要求为：

a) 不宜将不同数字化车间感知控制层生产系统的数据服务器软件安装在同一台主机上；各个生产系统网段的数据服务器不宜直接连接在同一个网络上；

b) 数字化车间感知控制层生产系统应提供监视和控制区域边界通信的能力，并提供入侵检测的能力；

c) 应限制物联网或无线网络与感知控制层相连；应提供默认拒绝所有外界网络数据流，例外允许网络数据流（也称为拒绝所有，允许例外）的能力；应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d) 对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为；

e) 数字化车间感知控制层安全域之间的边界防护机制失效时，及时进行报警；

f) 感知控制层与云平台相连时，应在感知控制层设置物理边界防护；

g) 对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

C.2.2 监控层增强要求

在数字化车间监控层对区域划分与边界防护的增强要求为：

a) 不宜将不同数字化车间监控层生产系统的数据服务器软件安装在同一台主机上；各个生产系统网段的数据服务器不宜直接连接在同一个网络上；

b) 数字化车间监控层生产系统应提供监视和控制区域边界通信的能力，并提供入侵检测与防御的能力；

c) 应限制物联网或无线网络与监控层相连；应提供默认拒绝所有外界网络数据流，例外允许网络数据流（也称为拒绝所有，允许例外）的能力；应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d) 对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为；

e) 数字化车间监控层安全域之间的边界防护机制失效时，及时进行报警；

f) 监控层与云平台相连时，应在监控层设置物理边界防护；

g) 对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

C.2.3 执行层增强要求

在数字化车间执行层对区域划分与边界防护的增强要求为：

a) 数字化车间执行层中的关键区域应限制物联网或无线网络与执行层相连，应限制任何云平台与执行层中关键区域相连；

b) 数字化车间执行层中的关键区域应提供监视和控制区域边界通信的能力，并提供入侵检测与防御的能力；

c) 应限制物联网或无线网络与执行层的关键区域相连；应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d) 数字化车间的执行层中的关键区域的边界防护机制失效时，及时进行报警；

e) 执行层与云平台相连时，应在执行层设置物理边界防护；

f) 对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

C.3 身份鉴别与认证

C.3.1 感知控制层增强要求

在数字化车间感知控制层对身份鉴别与认证的增强要求为：

a) 无线系统应具备识别接入设备并阻止未经授权的设备接入的能力；

b) 在无线系统无法提供上述能力的情况下，控制系统应具备识别与控制系统相连的无线系统的接入设备并阻止未经授权的设备接入的能力；

c) 若系统使用无线通讯，需使用加密的方式进行连接认证。

C.3.2 监控层增强要求

在数字化车间监控层对身份鉴别与认证的增强要求为：

a) 系统应提供访问用户身份认证的能力；

b) 系统应针对连续无效的访问尝试进行次数限制。当限制次数超出后，系统应在规定的周期内拒绝访问或者直到管理员解锁。

C.4 使用控制

C.4.1 感知控制层增强要求

在数字化车间感知控制层对使用控制的增强要求为：

a) 系统应提供建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施；

b) 系统应具备系统关键文件监控功能，防止关键文件被篡改；

c) 当系统通讯协议为动态端口时，系统应具备对动态端口相应的管理能力，以保证系统通讯的安全性；

d) 系统密码实现定期更改，防止密码长期不更改导致密码泄露。

C.4.2 监控层增强要求

在数字化车间监控层对使用控制的增强要求为：

a) 数字化车间生产系统应提供阻止接收来自生产系统外的用户或系统的个人间通信消息的能力；

b) 系统应定期更新杀毒软件；
c) 系统应具备系统关键文件监控功能，防止关键文件被篡改；
d) 应定期备份关键文件。

C.5 资源控制

C.5.1 感知控制层增强要求

在数字化车间感知控制层对资源控制的增强要求为：
a) 网络化的感知控制设备应提供检测和防范 DoS 事件的能力，并能避免 DoS 事件影响其他设备或网络；
b) 网络化的感知控制设备应提供能力：根据可配置的频率自动进行关键文件的备份。

C.5.2 监控层增强要求

在数字化车间监控层对使用控制的增强要求为：
a) 应在过程监控层安全网络与上层网络间部署入侵防护设备，能够监视边界处的常见网络攻击行为（包括端口扫描攻击、强力攻击、木马后门攻击、DoS 攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫等），并能够在检测到攻击行为时实时记录攻击源 IP、攻击类型、攻击目标、攻击时间，并提供报警；
b) 应提供能力：根据可配置的频率自动进行主机、服务器关键文件的备份。

C.5.3 执行层增强要求

在数字化车间执行层对使用控制的增强要求为：
a) 应能够监视接入该层网络的主机、服务器的网络负荷、流量、连接数、会话数、会话响应时间等网络资源信息；
b) 应能够监视接入该层网络的主机、服务器、软件程序及相关网络设备的运行状态，例如设备的 CPU 负荷、内存使用、硬盘使用情况警信息等；
c) 应动态监视软件进程占用的资源，提供限制资源使用的能力，防止资源耗尽；
d) 应提供能力：根据可配置的频率自动进行主机、服务器关键文件的备份。

C.6 数据安全

C.6.1 感知控制层增强要求

在数字化车间感知控制层对数据安全的增强要求为：
a) 系统应提供检测关键静态数据（如组态的工艺工程文件、存储的应用程序等）完整性被破坏的能力；
b) 系统应提供检测具备检查关键通信数据（如用户组态数据、上传/下载程序数据等）传输过程完整性被破坏的能力；
c) 系统应提供关键静态数据（如组态的工艺工程文件、存储的应用程序等）加密的能力；
d) 系统应提供关键通信数据（如组态的工艺工程文件、存储的应用程序等）加密的能力；
e) 感知控制层的设备应具有数据安全功能，并具有备份功能；
f) 应根据安全评估结果和要求，对感知控制层进行有针对性的数据的安全保护策略；
g) 应建立基于物理访问的安全分级保护机制；
h) 在组织安全和运营安全方面应根据安全分级，对数据安全进行管理；

i) 应从整个安全生命周期的角度，制定对感知控制层的数据安全策略；
j) 感知控制层数据应能够可靠传输至监控层或更高层。

C.6.2 监控层增强要求

在数字化车间监控层对数据安全的增强要求为：
a) 系统应提供检测关键静态数据（如组态的工艺工程文件、存储的应用程序等）完整性被破坏的能力；
b) 系统应提供检测具备检查关键通信数据（如用户组态数据、上传/下载程序数据等）传输过程完整性被破坏的能力；
c) 系统应提供关键静态数据（如组态的工艺工程文件、存储的应用程序等）加密的能力；
d) 系统应提供关键通信数据（如组态的工艺工程文件、存储的应用程序等）加密的能力；
e) 监控层的设备应具有数据安全功能，并具有备份功能；
f) 应根据安全评估结果和要求，对监控层进行有针对性的数据的安全保护策略；
g) 应建立基于物理访问的安全分级保护机制；
h) 在组织安全和运营安全方面应根据安全分级，对数据安全进行管理；
i) 应启用有效的数据安全方案，如冗余，带失效关闭的防火墙等机制。

C.6.3 执行层增强要求

在数字化车间执行层对数据安全的增强要求为：
a) 应减少或者避免受恶意软件攻击造成系统故障，提升系统可用性；
b) 应保护系统和数据的完整性，避免出现功能故障或者生产故障；
c) 应保护机密数据、信息和知识产权；
d) 应设置系统强化机制，进行认证和用户管理；
e) 应具备补丁管理机制；
f) 应具有攻击检测功能；
g) 应具备访问保护功能；
h) 应具有多层且一体化的保护机制。

C.7 安全审计

C.7.1 感知控制层增强要求

在数字化车间感知控制层对安全审计的增强要求为：
a) 应对嵌入式控制器内的修改事件（包括配置修改事件、算法修改事件、控制程序修改事件、关键变量修改事件等）和控制器服务事件（包括组态服务、数据块下载服务、程序下载服务、写服务等）进行安全审计，并生成审计报表进行分析；
b) 应根据系统的统一安全策略，实现集中审计，注意审计任务时钟保持与系统主时钟同步。

C.7.2 监控层增强要求

在数字化车间监控层对安全审计的增强要求为：
a) 应能够对关键系统中各类软/硬件设备的日志进行审计；
b) 根据系统资源许可情况，审计范围应覆盖到所有操作；
c) 应对审计进程进行保护，防止未经授权的中断。

C.7.3 执行层增强要求

在数字化车间执行层对安全审计的增强要求为：

a） 应能够对关键系统中各类软/硬件设备的日志进行审计；

b） 根据系统资源许可情况，审计范围应覆盖到所有操作；

c） 应对审计进程进行保护，防止未经授权的中断。

参 考 文 献

[1] GB/T 20720.2—2020 企业控制系统集成 第2部分:企业控制系统集成的对象和属性

[2] GB/T 20720.3—2010 企业控制系统集成 第3部分:制造运行管理的活动模型

[3] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[4] GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

[5] GB/T 33009.4—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第4部分:风险与脆弱性检测要求

[6] IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3:System security requirements and security levels