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。