ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41257—2022

数字化车间功能安全要求

Functional safety 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

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、浙江中控技术股份有限公司、北京和利时系统工程有限公司、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、中国科学院沈阳自动化研究所、上海工业自动化仪表研究院有限公司、上海自动化仪表有限公司、中石化广州工程有限公司、长沙有色冶金设计研究院有限公司、北京市劳动保护科学研究所。

本文件主要起草人：孟邹清、史学玲、郭苗、魏振强、裘坤、王志平、熊文泽、朱杰、刘盈、田雨聪、文科武、徐皑冬、周有铮、杨明、王敏良、马百旺、闫炳均、靳江红、李佳、彭小波、马欣欣、冯健、陈汝、牛海明、鄢锋、杨静雅、谢亚莲、陆妹、张亚彬、张雪、姜瑞景。

引　言

数字化车间是智能制造的核心单元，涉及领域广泛，类型复杂多样。智能化技术在给制造业带来难得发展机遇的同时，也使制造业面临着安全方面的挑战。数字化车间中存在多种风险，面临多种安全问题，如：数字化制造设备的运行失效（包括控制功能失效、安全功能失效），可能会导致制造系统的功能失控、产品质量下降等，从而对周围的人员、资产或环境造成危害，带来巨大的经济损失，造成声誉方面的影响。

《中国制造 2025》纲要明确提出要建立智能制造安全保障系统。为了降低数字化车间中的风险，保障数字化车间的安全运行，需采用功能安全的技术手段，通过危险与风险分析、保护层评估，明确数字化车间的功能安全要求，在数字化车间中设置保护层（如：安全相关系统、物理保护系统等），建立功能安全管理系统，全方位多角度保障数字化车间的功能安全。

依据 GB/T 37393—2019《数字化车间　通用技术要求》，数字化车间重点涵盖产品生产制造过程，其体系结构分为基础层和执行层。因此，本文件中数字化车间的功能安全要求也将限定在基础层和执行层的范围内。

数字化车间的功能安全，主要考虑以下三个方面。

一是针对数字化车间中已识别的危险及风险分析结果，结合行业或企业自身的可容忍风险，进行保护层评估，确定各类保护措施的必要性以及所需的安全保护功能。在数字化车间的基础层中设置适当保护层（如：安全相关系统、物理保护系统等），用以降低数字化车间生产过程中可能带来的对资产、人员、环境产生的风险。尤其针对数字化车间自身特点，重点关注车间的制造设备或装置在互相联通后带来的新的风险，以及由于数字化、网络化、智能化的升级促成实现的安全保护新模式。

二是在数字化车间的执行层中建立一个功能安全管理信息系统，对数字化车间的安全风险、保护层、安全相关系统以及其他功能安全相关活动进行数据采集分析、可视化管理、动态管控。

三是构建一个功能安全信息物理系统，通过 E/E/PE 安全相关系统、其他风险减低措施和功能安全管理信息系统等的有机融合与深度协作，实现数字化车间功能安全的实时感知、动态控制和信息服务。

功能安全信息物理系统，包括：

——基础层的 E/E/PE 安全相关系统（包含安全检测、控制和执行）、其他风险减低措施及其检测单元、安全服务器、安全接口和通信；

——执行层的功能安全管理信息系统及其安全数据、服务等。

数字化车间功能安全的示意图，如图 1 所示。

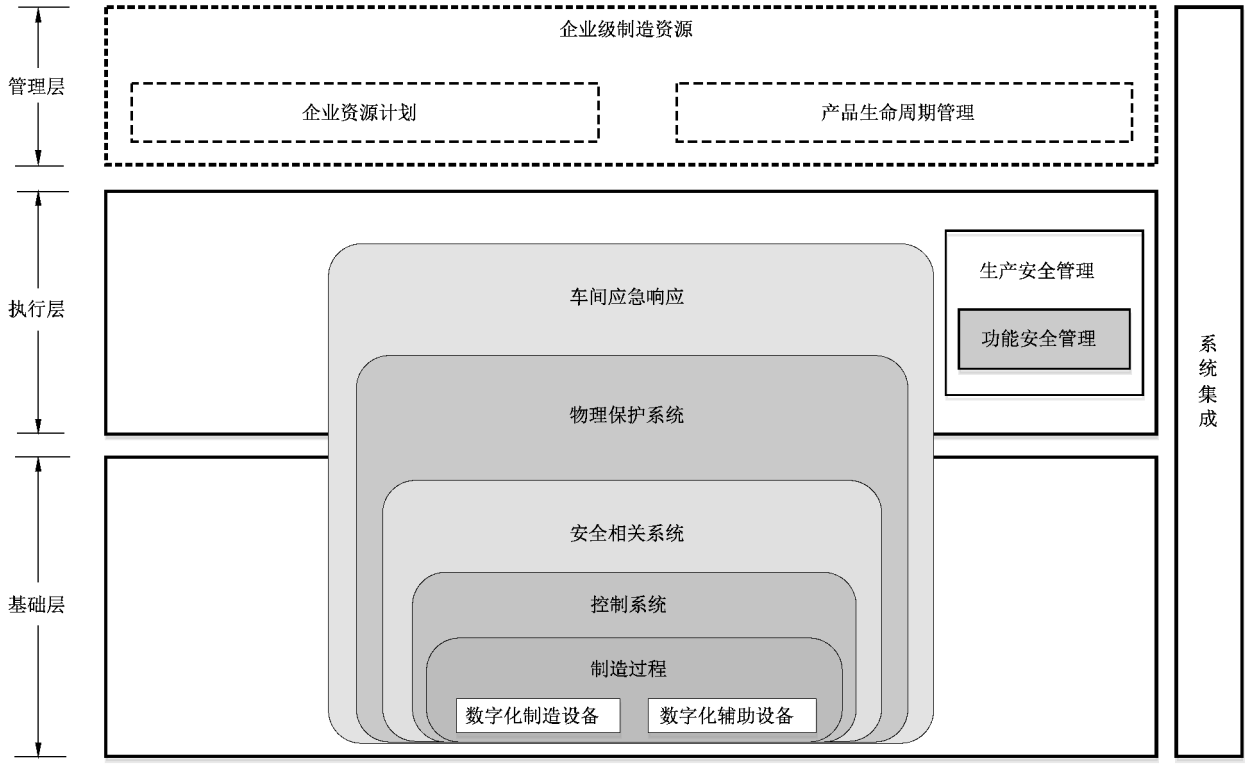

图 1　数字化车间功能安全示意图

数字化车间功能安全相关活动的过程和结果，通过采用计算机可识别的形式采集、存储、调用、处理和展示，以实现完整记录、保存以及可追溯，适应数字化车间建设需要。

数字化车间功能安全要求

1 范围

本文件规定了安全生命周期、数字化车间的功能安全管理、数字化车间危险与风险分析、数字化车间保护层评估、安全相关系统要求、功能安全管理信息系统要求、功能安全集成要求等内容。

本文件适用于指导数字化车间的新建和改扩建。

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 20438.1 电气/电子/可编程电子安全相关系统的功能安全 第1部分：一般要求

GB/T 20438.2 电气/电子/可编程电子安全相关系统的功能安全 第2部分：电气/电子/可编程电子安全相关系统的要求

GB/T 20438.3 电气/电子/可编程电子安全相关系统的功能安全 第3部分：软件要求

GB/T 20438.4 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 37393—2019 数字化车间 通用技术要求

GB/T 37413—2019 数字化车间 术语和定义

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20438.4 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

控制系统 control system

响应来自过程和(或)操作者的输入信号，并产生输出信号，使制造过程按预期方式工作的系统。

[来源：GB/T 20438.4—2017，3.3.3，有修改]

3.1.3

制造执行系统 manufacturing execution system

生产活动管理系统，该系统能启动、指导、响应并向生产管理人员报告在线、实时生产活动的情况。这个系统辅助执行制造订单的活动。

[来源：GB/T 25486—2010，2.162]