ICS 25.160.01
CCS J 33

CWA

团　　体　　标　　准

T/CWAN 0173—2025

大模型技术应用于焊接工艺优化规范

Standards for the application of large-scale model technology in welding process optimization

2025-11-17 发布　　2025-12-01 实施

中国焊接协会　发布

目　　录

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。

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。

本文件由中国焊接协会提出并归口。

本文件起草单位：北京博清科技有限公司、安徽博清机器人科技有限公司、中国兵器工业集团航空弹药研究院有限公司、北京理工大学（珠海）、上海中巽科技股份有限公司、广西柳工机械股份有限公司、天津市特种设备监督检验技术研究院、哈尔滨职业技术大学、北部湾大学、哈尔滨中焊协学技术服务有限公司、福建省特种设备检验研究院、哈尔滨华德学院、坤智大数据科技（哈尔滨）有限公司。

本文件主要起草人：冯消冰、韩滕跃、郭涛、韩冬、李海龙、侯国清、王铭秋、牛卫飞、潘百蛙、崔元彪、范东辉、王东宝、李超月、黎泉、方乃文、汪路奇、林晓辉、郑桂红、孙明辉、李长威、于修和。

大模型技术应用于焊接工艺优化规范

1 范围

本文件规定了大模型技术应用于焊接工艺优化的规范的术语和定义、数据要求、技术要求、优化能力评估等内容。

本文件适用于大模型技术应用于焊接工艺优化，包括焊接质量提升、焊接效率提升、焊接成本控制、工艺稳定性提升四个主要方面。

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 3375 焊接术语

GB/T 2651 金属材料焊缝破坏性试验 横向拉伸试验

GB/T 42127—2022 智能制造 工业数据 采集规范

GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求

3 术语和定义

GB/T 3375-1994 焊接术语界定的及下列术语和定义适用于本文件。

3.1

工艺设计优化 process design optimization

通过系统性调整生产流程、参数及资源配置，实现效率提升、成本降低和质量改进的技术活动。

3.2

焊接路径规划 welding path planning

根据焊接工件的焊缝特征、机器人运动学特性、焊接工艺要求及环境约束，用算法确定机器人末端执行器（焊枪）从起点到终点的最优运动轨迹。

3.3

焊接质量评估 weld quality assessment

是对焊接成果的完整性、可靠性及安全性进行评估的技术流程。

3.4

工艺稳定性 process stability

焊接工艺在重复执行过程中保持关键质量特性与效率指标一致性的能力。

4 数据要求

4.1 数据内容要求

大模型技术在焊接工艺优化中对数据的要求主要包括数据规模、数据质量和数据多样性。

4.1.1 数据规模

大模型需要数据进行训练和优化。在焊接工艺优化中，数据规模的要求体现在以下几个方面：

a）历史焊接记录：历史焊接记录作为训练数据，需要数万组甚至更多的数据来训练模型，以确保模型的准确性和泛化能力；

b）实时采集的数据：在焊接过程中，需要实时采集焊接数据，如电参数、机器人运动参数、形状参数（原始坡口和每层及每道焊后形状参数）等；

c）焊接知识库：包含焊接领域各种知识和信息的资源集合；

d) 焊接质量数据：焊接质量数据是焊接大模型优化工艺、判断质量的核心依据，需覆盖 “缺陷检测、性能指标、质量评定”等。

4.1.2 数据质量

高质量的数据是确保模型准确性的关键。在焊接工艺优化中，数据质量的要求包括：

a）数据准确性：采集的数据需要准确反映焊接过程中的各种参数和状态，采集偏差控制在 1-3%以内。

b）数据完整性：所有关键参数和数据都需要完整记录保存，如电参数、机器人运动参数、形状参数（原始坡口和每层及每道焊后形状参数）等。

c）数据一致性：不同批次和不同设备采集的数据需要保持一致性，确保模型训练的稳定性和可靠性。

d）数据边界性：数据不能单一存在，要有范围，能够确保大模型在工艺优化过程中具有一定的工艺窗口。

4.1.3 数据多样性

数据的多样性有助于提高模型的泛化能力，适应不同的焊接场景和条件。在焊接工艺优化中，数据多样性的要求包括：

a）多种焊接条件：需要涵盖不同的焊接条件，如不同的材料、不同的焊接方法和不同的工艺参数；

b）异常情况处理：需要包含异常情况的数据，如焊接过程中的各种异常现象和问题，以便模型能够识别和处理这些情况；

c）多源数据融合：需要将多种来源的数据进行融合，如光谱分析仪监测的焊接烟尘成分、工人操作姿势稳定性等。

4.2 数据格式要求

数据格式总体要求宜符合 GB/T 42127—2022 的数据采集要求。

4.2.1 用于预训练或微调的数据宜满足的数据格式如下：

a) 工艺参数数据格式：结构化表格（如 CSV、JSON、Parquet），数值型字段需标注单位，缺失值以 NULL 或 NA 标识；

b) 传感器时序数据格式：时间序列数据（如 HDF5、TFRecord）,时间戳精度≥1ms，通道数据需标注采样频率（如 10kHz）；

c) 视觉/图像数据格式：无损压缩图像（如 PNG）或视频流（如 H.264 编码的 MP4）；

d) 材料属性数据格式：如 JSON 或 XML；

e) 输出的优化建议数据格式：如结构化 JSON；

f) 优化建议输出需包含置信度评分与约束条件。

5 技术要求

5.1 功能要求

5.1.1 具备工艺设计优化功能

焊接大模型在工艺设计阶段，具备的优化能力包含但不限于：

a）参数推荐（例如：电流、电压、速度、保护气体配比等）；

b）焊接路径规划（例如：如机器人焊接轨迹优化）；

c）材料匹配（例如：母材与焊材的兼容性分析）。

5.1.2 具备生产过程控制优化功能

焊接大模型在生产过程控制阶段，具备的优化能力包含但不限于：

a）实时监测与参数动态调整（例如：基于传感器数据反馈）；

b）缺陷预测与预警（例如：通过视觉或声学信号识别）。

5.1.3 具备后处理与评估优化功能

焊接大模型在后处理与评估阶段，具备的优化能力包含但不限于：

a）焊缝质量评估（例如：基于 X 射线、超声波等检测数据）；

b) 工艺改进建议（例如：历史数据挖掘）。

5.2 模型优化要求

5.2.1 模型优化总体要求

a) 科学性

1) 所有优化建议必须基于焊接机理与数据驱动的双重验证，符合材料科学、热力学、冶金学等基础理论，避免黑盒推荐。

2) 关键参数（如热输入、冷却速率）需在物理可行范围内。

b)安全性与可靠性

1) 优化建议不得突破工艺安全边界（如设备承压极限、材料热影响区临界值）。

2) 涉及高风险场景（如压力容器焊接）时，需人工复核。

c) 可解释性与透明度

1)模型需提供优化建议的逻辑依据（如特征重要性分析、关键数据关联性），支持工程师理解与验证。

d) 动态适应性

1)针对生产环境变化（如材料批次差异、设备磨损），模型宜具备在线学习或增量更新能力，避免静态规则失效。

e) 经济性平衡

1) 优化方案需综合评估质量、效率、成本最优。

2) 明确成本节约的量化预期（如能耗降低≥5%）。

f)合规性与标准化

1) 所有建议需符合现行焊接标准（如 ISO、AWS、GB）的强制性要求，并标注与标准的符合性条款。

2) 数据输入与输出需满足大模型行业数据安全规范（如脱敏处理、权限管控）。

5.2.2 焊前阶段：工艺设计优化要求

a) 能够存储大量的焊接工艺标准和规范，包括不同材料（如碳钢、不锈钢、铝合金等）之间的焊接参数（电流、电压、焊接速度等）。

b) 系统可以根据工件的材料和结构特点，快速推荐合适的焊接工艺。提供最佳的焊接参数、运动参数和焊道排布等。

c) 大模型技术可以通过分析历史数据与实时反馈，调整焊接过程中的电流、电压、速度等关键参数，确保获得最理想的焊接效果。能够根据材料特性和环境变化自动调整焊接条件，提高焊接质量与效率。

5.2.3 焊中阶段：生产过程控制优化要求

a) 识别生产计划，对焊接任务进行分解，确定每个任务所需的焊接工艺、设备和人员数量。实时监控生产进度，当出现意外情况（如设备故障或人员缺勤）时，快速调整生产计划。

b) 通过连接焊接设备上的传感器，系统可以获取实际的焊接参数，并与设定的工艺参数进行对比。如果发现偏差超出允许范围，系统会及时发出警报，提醒操作人员进行调整，从而确保焊接质量的一致性。

c) 自主预测坡口形状、装配尺寸、焊道排布情况对焊缝致密性的影响，可以自主预测焊接电参数、运动参数等对焊缝性能的影响，可以自动识别焊缝无损检测中的缺陷，进一步提高检测的准确性和效率。

5.2.4 焊后阶段：后处理与评估优化要求

a)对于焊接接头内部缺陷（如气孔、夹渣、裂纹等），系统能够根据检测数据进行判断，并对缺陷严重程度进行分级。另一方面，系统还会对焊接质量数据进行统计分析，找出影响焊接质量的关键因素。

5.3 **安全与隐私要求**

总体上宜遵循 GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求中 4 训练数据

安全要求、5 模型安全要求、6 安全措施要求中的内容。

5.3.1 大模型技术的安全要求主要包括以下几个方面：

a）数据安全要求

1）信息来源安全

信息来源管理方面，要求使用合法来源的信息，并对信息内容质量提出了量化标准，如信息内容不良信息超过 5%的，不宜采集或使用该来源信息。信息来源搭配方面，要求提高信息来源的多样性。信息来源可追溯方面，要求数据提供者具备合法合规的处理依据。

2）信息内容安全

知识产权合规方面，要求建立知识产权管理策略、识别知识产权侵权风险、完善投诉举报渠道、公开摘要信息等。

个人信息保护方面，要求服务提供者宜确保其个人信息处理行为具有合法性基础，即取得对应个人信息主体的同意或符合法律、行政法规规定的其他情形。当涉及敏感个人信息的使用时，还必须获得个人的单独同意。

3）信息标注安全详细内容见表 1。

表 1 信息标注安全表

类别	要点	具体要求
标注人员	安全培训	定期对标注人员进行培训，培训内容包括标注任务规则、标注工具使用方法、标注内容质量核验方法、标注数据安全管理要求等
	考核	考核合格者具备上岗资格，考核内容包括标注规则理解能力、标注工具使用能力、安全风险判定能力、数据安全管理能力等
		建立定期重新培训考核以及必要时暂停或取消标注上岗资格的机制
	职能划分	至少划分为数据标注和数据审核两类，同一标注任务下同一人员不得担任多项职能
标注规则	规则制定	标注规则包括标注目标、数据格式、标注方法、质量指标等内容，覆盖数据标注以及数据审核等环节
	功能性标注规则	宜能指导标注人员按照特定领域特点生产具备真实性、准确性、客观性、多样性的标注信息
	安全性标注规则	宜能指导标注人员围绕信息及生成内容的主要安全风险进行标注
标注内容准确性	人工抽检	对于功能性标注，对每一批标注信息采取人工抽检，内容不准确的，宜重新标注；内容中包含不良信息的，该批次标注信息应作废
	逐条审核	对于安全性标注，每一条标注信息至少经由一名审核人员审核通过

b）模型安全要求

1）模型生成内容安全性：要求服务提供者宜对每次使用者输入的信息进行安全性监测，并建立常态化检测测评手段，对测评过程中发现的安全问题及时处置，通过指令微调、强化学习等方式优化模型。

2）模型生成内容准确性：要求服务提供者采用技术手段提高生成内容的实时性与精准度。

3）模型生成内容可靠性：要求服务提供者采取技术措施提高生成内容格式框架的合理性以及有效内容的含量，提高生成内容对使用者的帮助作用。

c）安全措施要求

1）模型适用性

在服务范围内应用人工智能生成内容（AIGC）时宜充分论证模型的必要性、适用性和安全性。

2）服务透明度

在显著位置向社会公开服务适用的人群、场合、用途等信息，并公开基础模型使用情况。以可编程接口形式提供服务的，宜在说明文档中公开上述信息。

3)用户数据处理

服务提供者宜为用户提供便捷途径关闭输入信息用于模型训练的功能，如设置易懂选项或简洁语音控制指令。为确保便捷性，通过选项关闭时，操作过程宜控制在四次点击以内。同时，服务提供者宜确保界面设计或用户交互中显著告知信息收集状态，并清晰展示关闭选项或指令，以符合“透明度”要求。

4)用户管理

实施监测机制：通过关键词筛查或分类模型等方式，对用户输入的信息进行实时监测，以便及时发现并处置不当行为。

拒绝回答机制：对于检测到违反《生成式人工智能服务安全基本要求》附录 A 要求的问题，服务提供者的系统应自动拒绝回答。

人工监看机制：配备专门的监看人员，及时根据监看情况提升生成内容的质量与安全性，并对第三方投诉进行收集和响应。

5)服务稳定性

为维护服务稳定性，服务提供者应采取安全措施。持续监测模型输入内容，预防恶意攻击。定期安全审计，识别和修复安全漏洞。建立数据、模型备份和恢复策略。

d）安全评估要求

为确保评估工作的可操作性，针对信息安全、生成内容安全、问题拒答等方面提出了量化的评估标准，具体要求请见表 2。

表 2 安全评估要求表

序号	评估事项	具体要求
1	信息安全	采用人工抽检，从全部信息中随机抽取不少于4000条信息，合格率不宜低于96%
		结合关键词、分类模型等技术抽检，从全部信息中随机抽取不少于总量10%的信息，抽样合格率不宜低于98%
		评估采用的关键词库、分类模型宜符合GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求第6章要求
2	生成内容安全	建设符合GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求 B.1.2要求的生成内容测试题库
		采用人工抽检，从生成内容测试题库中随机抽取不少于1000条测试题，模型生成内容的抽样合格率不宜低于90%
		采用关键词抽检，从生成内容测试题库中随机抽取不少于1000条测试题，模型生成内容的抽样合格率不宜低于90%
		采用分类模型抽检，从生成内容测试题库中随机抽取不少于1000条测试题，模型生成内容的抽样合格率不宜低于90%

3	问题拒答	建设符合GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求 B.1.3要求的拒答测试题库
		从拒答测试题库中随机抽取不少于300条测试题，模型的拒答率不宜低于95%
		从非拒答测试题库中随机抽取不少于300条测试题，模型的拒答率不宜高于5%

5.3.2 大模型技术的隐私要求主要包括以下几个方面：

a）数据安全和隐私保护

1）数据脱敏处理：对敏感数据进行脱敏处理，防止直接暴露原始数据。

2）加密传输与存储：采用加密技术对数据进行传输和存储，防止数据在传输和存储过程中被窃取或篡改。

3）联邦学习框架：在联邦学习框架下，各参与方在本地设备上进行模型训练，只交换模型参数而非原始数据，从而保护本地数据隐私。

4）差分隐私机制：在数据处理过程中添加噪声，保护隐私信息，同时不影响模型训练效果。

b）模型安全和隐私保护技术

1）模型加密技术：通过对模型参数进行加密处理，防止模型被非法访问或篡改。

2）模型水印技术：将特定的标识信息嵌入到模型中，用于追踪模型的非法使用。

3）访问控制策略：设置严格的访问控制策略，基于角色的访问控制(RBAC)模型，明确不同角色对模型服务的访问权限。

c）对抗攻击和后门攻击的防范

1）对抗攻击：通过构造的输入欺骗大模型，产生错误输出。

2）后门攻击：在训练过程中嵌入特定漏洞，通过特定输入操纵模型输出。

3）提示词攻击：利用大模型对提示词的敏感性实施攻击，诱导模型产生错误输出或泄露敏感信息。

d）内容合规问题

1）版权侵权：避免未经授权使用他人作品或复制他人内容。

2）虚假信息：确保生成的内容真实可靠，避免虚假信息的传播。

3）低俗内容：避免生成低俗、不良内容，确保内容健康向上。

5 优化能力评估

6.1 评估数据集

6.1.1 工艺设计优化数据集构成要求

a) 数据内容：

1) 历史工艺参数库（例如焊接电流、焊接电压、焊接速度、气体配比等）；

2) 材料组合数据（例如母材牌号、焊材型号/牌号、厚度、力学性能等）；

3) 设计目标（例如强度≥X MPa、变形量≤Y mm 等）；

4) 成功与失败案例标签（例如焊缝成形评分 1~5 级等）。

b) 数据量：

1)需覆盖焊接方法（例如 MIG、TIG、MAG 等），每种方法≥1000 组有效数据；

2) 材料组合覆盖常用材料。

6.1.2 生产过程控制优化数据集构成要求

a) 数据内容：

1) 实时传感器数据（例如电流/电压波动、温度场、振动信号等）；

2) 设备状态日志（例如送丝速度、冷却水温度等）；

3) 过程异常记录（例如飞溅、弧光中断时间戳等）；

4) 同步采集的焊缝图像/视频（例如标注缺陷位置与类型等）。

b) 数据量：

1) 连续生产数据时长≥200 小时；

2) 至少包含 5 类典型异常场景（例如气孔、未熔合等）。

6.1.3 后处理与评估优化数据集构成要求

a)数据内容：

1)无损检测结果（例如 X 射线、超声波检测原始数据与报告）；

2)破坏性试验数据（例如拉伸、冲击试验值）；

3)工艺改进反馈（例如人工修正后的参数与效果对比）。

b) 数据量：

1)每种检测方法≥500 组数据，标注缺陷类型与尺寸（例如气孔直径≤0.5mm）；

2)破坏性试验宜按照 GB/T 2651 等进行。

6.2 **评估方法**

采用以下两种评估方法：

6.2.1 人工评估

大模型推广之前，宜采用相关领域焊接高技能人员在预部署阶段评估大模型应用的输出水平，进行交叉验证，进根据综合表现进行整体打分。

6.2.2 用户反馈

大模型推广之后，通过相关功能来收集用户反馈，例如：对于模型的输出工艺的焊接效果，可以评估为良好、一般和不合格三种情况。