ICS 35.240.50
CCS L 70

团 体 标 准

T/CEATEC XXX—2025

流程工业云边端系统可靠性评估规范

Specifications for reliability assessment of cloud-edge-terminal system in process industry

（征求意见稿）

2025-X-XX 发布 2025-X-XX 实施

中国欧洲经济技术合作协会 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。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次编制。

流程工业云边端系统可靠性评估规范

1 范围

本文件规定了流程工业云边端系统可靠性评估的评估总则、可靠性指标体系、评估方法与模型、评估实施与报告。

本文件适用于流程工业领域的云边端协同系统可靠性评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

流程工业 process industry

以连续或间歇式生产方式，通过物料的物理、化学变化实现产品生产的工业领域，包括化工、石化、冶金、电力、建材等行业，其生产过程具有连续性、实时性、高安全性要求的特征

4 评估总则

4.1 评估目的

通过建立科学、统一的可靠性评估体系，量化流程工业云边端系统的可靠性水平，识别系统设计、运行、维护过程中的可靠性薄弱环节，提出针对性的改进措施，保障流程工业生产的连续性、稳定性和安全性，降低系统故障导致的生产损失。

4.2 评估原则

4.2.1 科学性原则

评估指标、方法和流程应符合现行国家标准和工业技术规范，基于流程工业生产特性和云边端系统技术架构设计，确保评估结果的科学性和客观性。

4.2.2 系统性原则

评估覆盖流程工业云边端系统的端、边、云各层级及各层级间的协同环节，兼顾硬件设备、软件系统、网络传输等各组成部分的可靠性。

4.2.3 可操作性原则

评估指标应可量化、可采集，评估方法应简便易行，评估流程应标准化，适配流程工业企业和第三方评估机构的实际应用需求。

4.2.4 场景化适配原则

针对流程工业不同行业的生产场景（如化工连续生产、冶金间歇生产），可对评估指标阈值进行合理调整，确保评估结果贴合实际生产需求。

4.3 评估基本要求

4.3.1 评估所需的系统运行数据、故障记录、设备参数等资料应真实、完整、有效，数据采集周期不应少于90天。

4.3.2 评估人员应具备流程工业生产工艺、云边端技术、系统可靠性评估等相关专业知识和实践经验。
4.3.3 评估结果应进行多维度验证，确保数据准确、结论可靠，评估全过程应形成可追溯的记录。

4.4 评估流程

总体流程包括六个阶段，各阶段的主要工作内容如下：

a）评估准备阶段：明确评估目标、范围和边界；组建具备多学科知识的评估团队；收集系统架构图、设计文档、运维记录、故障历史等基础资料；

b）指标体系构建阶段：根据系统特点和评估目标，选择并细化适用的可靠性指标，确定各指标的采集方法、计算方式和目标值；

c）数据采集与处理阶段：采集规定周期内的系统运行数据、故障数据和性能数据，对数据进行清洗、校验、归一化和统计分析；

d）评估模型应用阶段：根据系统架构复杂度和数据情况，选择合适的评估方法与模型，进行定量计算和定性分析；

e）结果分析与评级阶段：综合评估结果，确定系统的可靠性等级，识别系统可靠性薄弱环节和关键风险点；

f）报告编制与改进阶段：编制详细的可靠性评估报告；提出针对性的设计改进、运维优化或管理提升建议，并跟踪改进效果。

5 可靠性指标体系

5.1 指标构成

流程工业云边端系统可靠性指标体系分为三个层次：

a）系统级指标：反映云边端系统作为整体对外提供服务的可靠性水平；

b）层级/组件级指标：针对云端平台、边缘节点、端设备和通信网络分别设定；

c）基础指标：计算其他指标的底层参数，如MTBF、MTTR等。

注：评估时可根据具体对象选取全部或部分指标：

5.2 系统级指标

系统级核心指标、定义及目标要求见表1。

表1 系统级可靠性核心指标

指标名称	符号	定义	单位	目标值参考
系统可用性	A_s	系统处于可执行所有规定功能状态的概率	%	≥99.95
关键任务成功率	TSR_k	成功完成的关键业务任务数占总提交数的比率	%	≥99.5
端到端数据完整率	DIR_e2e	从端设备到云端，数据被完整无误接收的比率	%	≥99.99
系统平均无故障工作时间	$MTBF_s$	系统级服务中断故障间的平均工作时间	h	≥720
系统平均恢复时间	$MTTR_s$	系统从故障发生到完全恢复的平均时间	h	≤2

5.3 层级/组件级指标

5.3.1 云端平台指标

云端平台核心指标及目标要求见表2。

表2 云端平台可靠性核心指标

指标名称	符号	定义	单位	目标值参考
服务可用性	A_c	云服务可访问并提供功能的时间比率（依据 SLA）	%	≥99.99
API 响应时间(P95)	RT_{api}	95%的云端关键 API 调用响应时间	ms	≤200

指标名称	符号	定义	单位	目标值参考
数据持久性	R_{store}	数据在云存储中一年内不丢失的概率	%	≥99.999
虚机无计划重启率	λ_{vm}	虚拟机/容器非计划性重启的频率	次/(实例·年)	≤1

5.3.2 边缘节点指标

边缘节点核心指标及目标要求见表3。

表3 边缘节点可靠性核心指标

指标名称	符号	定义	单位	目标值参考
节点平均无故障工作时间	$MTBF_e$	边缘节点硬件/核心软件故障间的平均工作时间	h	≥8760
处理时延	$Latency_e$	数据在节点内完成处理所需的平均时间	ms	≤50
任务处理丢包率	PLR_e	边缘处理任务失败或超时丢弃的比率	%	≤0.1
资源可用率	RA_e	CPU/内存等关键资源处于可用状态的时间比率	%	≥99.9

5.3.3 端设备指标

端设备核心指标及目标要求见表4。

表4 端设备可靠性核心指标

指标名称	符号	定义	单位	目标值参考
设备平均无故障工作时间	$MTBF_d$	端设备故障间的平均工作时间	h	≥43800
数据采集准确率	AR_d	设备输出数据与标准值一致的比例	%	≥99.9
设备在线率	OR_d	设备与上级系统保持有效通信的时间比率	%	≥99.5
指令执行成功率	CSR_d	控制指令被成功接收并执行的比例	%	≥99.9

5.3.4 通信网络指标

通信网络核心指标及目标要求见表5。

表5 通信网络可靠性核心指标

指标名称	符号	定义	单位	目标值参考
网络可用性	A_n	关键通信路径（如端-边、边-云）通畅的时间比率	%	≥99.9
网络平均时延	$Latency_n$	数据包在关键路径上传输的平均时间	ms	≤100
网络丢包率	PLR_n	关键路径上丢失数据包的比例	%	≤0.5
网络抖动	$Jitter_n$	网络时延的变化量（标准差）	ms	≤20

5.4 基础指标

基础指标是用于理论建模与分析的根本参数，见表6。

表6 可靠性基础指标

指标名称	符号	定义与说明	单位
平均无故障工作时间	$MTBF$	可修复系统相邻故障间工作时间的期望值	h
平均修复时间	$MTTR$	系统故障后恢复至正常所需时间的期望值	h
故障率	λ	单位时间内发生故障的概率（指数分布下$\lambda=\frac{1}{MTBF}$）	1/h
可靠度	$R(t)$	系统在时间 t 内无故障运行的概率（指数分布下 $R(t)=e^{-\lambda t}$）	—
维修率	μ	单位时间内完成修复的概率（$\mu=\frac{1}{MTTR}$）	1/h

6 评估方法与模型

6.1 通用要求

应根据评估目的、系统架构复杂程度、数据完备性等因素，选择一种或多种评估方法与模型。鼓励采用定量模型进行核算，在数据不足时可结合专家打分、故障模式与影响分析（FMEA）等定性或半定量方法。

6.2 可靠性框图法

6.2.1 方法描述

将系统分解为若干功能单元（块），根据各单元在可靠性逻辑上的关系（串联、并联、混联等）绘制可靠性框图（RBD），然后根据框图模型计算系统可靠度或可用性。

6.2.2 建模步骤

按照以下步骤进行：

a）系统分解：根据系统功能逻辑，将其分解为相对独立的单元（如：云端集群、边缘节点A、边缘节点B、核心网络交换机、现场控制单元等）；

b）确定逻辑关系：分析各单元的功能依赖性，若所有单元均正常系统才正常，则为串联；若至少一个单元正常系统即正常，则为并联（冗余）；

c）绘制RBD：使用标准图形符号绘制框图；

d）计算系统可靠性：

——串联系统可靠度：$R_s(t)=\prod_{i=1}^{n} R_i(t)$；

——并联系统可靠度：$R_s(t)=1-\prod_{i=1}^{n}$（$1-R_i(t)$）；

——混联系统可靠度：综合运用串并联公式逐步计算。

注：系统可用性A_s可类比计算，用A_i替换$R_i(t)$。

6.3 马尔可夫模型

6.3.1 方法描述

适用于具有冗余配置、故障修复、多种工作状态及状态转移的系统。用状态表示系统可能的配置情况（如：双机热备、一主一备、降级运行等），用转移率（故障率λ、修复率μ）描述状态间的随机转移过程，通过求解稳态概率计算系统可用性。

6.3.2 建模步骤

按照以下步骤进行：

a）定义系统状态：列举系统所有可能的状态（如：状态0：双机正常；状态1：主机正常，备机故障；状态2：主机故障，备机正常；状态3：双机故障）；

b）绘制状态转移图：用圆圈表示状态，带箭头的线表示状态转移，并标注转移率；

c）建立状态转移率矩阵Q；

d）求解稳态概率向量π：通过方程组$\pi Q=0$且$\sum \pi_i=1$求解；

e）计算系统可用性：将所有代表系统可工作状态的稳态概率相加。

6.4 基于蒙特卡洛仿真的评估

6.4.1 方法描述

通过计算机随机抽样，模拟系统各组件在寿命周期内随机的故障和修复事件序列，通过大量重复实验（通常≥10000次），统计系统级可靠性指标（如$MTBF_s$，A_s）的分布情况。适用于复杂系统、非指数分布、复杂维修策略等场景。

6.4.2 仿真步骤

按照以下步骤进行：

a）建立组件模型：为每个组件定义故障时间分布（如指数分布、威布尔分布）和修复时间分布；

b）定义系统逻辑：明确系统的可靠性逻辑（串联、并联等）和故障判据；

c）设定仿真参数：总仿真时间T_{total}（如10年），仿真次数N_{sim}；

d）运行仿真：$Fori$=1 to N_{sim}，生成各组件在T_{total}内的故障和修复事件时间线，根据系统逻辑，合成系统级事件时间线（故障、恢复），统计本次仿真的系统累计不可用时间$T_{d,i}$、故障次数$N_{f,i}$；

e）结果分析：通过计算$MTBF_s=\frac{T_{total}-N_{sim}}{\sum N_{f,i}}$，$A_s=1-\frac{\sum T_{d,i}}{T_{total}\times N_{sim}}$可输出指标的置信区间。

6.4.3 适用场景

系统架构复杂，含有冷备、温备、优先级切换等机制；组件寿命不服从指数分布；需要考虑计划性维护与突发性维修的交互影响。

6.5 数据驱动评估方法

6.5.1 方法描述

基于系统历史运行数据，运用统计学和机器学习方法进行可靠性分析和预测。

6.5.2 主要方法

按照以下方法进行：

a）趋势分析：绘制关键组件故障率、MTTR等指标随时间（或运行循环次数）的变化曲线，识别性能退化趋势。可使用线性回归、指数平滑等方法；

b）相关性分析：分析环境变量（温度、湿度、电压波动）、负载率与故障发生之间的相关性（如Pearson相关系数、Spearman秩相关系数）；

c）预测性模型：

——时间序列模型：如自回归积分滑动平均模型（ARIMA），用于预测未来一段时间内系统或组件的故障次数或可用性趋势；

——生存分析模型：如Cox比例风险模型，用于分析多个协变量对设备故障风险的影响；

——机器学习模型：如基于长短期记忆网络（LSTM）的故障预测模型，利用多维历史序列数据预测剩余使用寿命（RUL）。

6.6 评估模型选择指南

根据系统特点和评估阶段，按表7选择评估模型。

表7 可靠性评估模型选择指南

系统特点/评估阶段	推荐模型	理由与说明
架构简单，逻辑清晰（设计阶段）	可靠性框图法	计算简便，能快速预估系统可靠性，指导冗余设计
含动态冗余与修复（设计/运维）	马尔可夫模型	能精确描述冗余切换、修复过程对可用性的提升
架构复杂，含多种分布与策略	蒙特卡洛仿真	灵活，可模拟随机过程，处理复杂逻辑和非标准分布
拥有丰富历史运行数据（运维阶段）	数据驱动方法	基于实际数据，可发现潜在规律，实现精准预测和预警
初步筛选或快速评估	可靠性框图法 结合专家打分	在数据不足时提供定性或半定量参考

7 评估实施与报告

7.1 评估准备

7.1.1 明确评估目标与范围

应明确本次评估是适用于设计验证、竣工验收、定期巡检还是故障后分析，并清晰界定被评估系统的物理和逻辑边界（如包含哪些云端服务、哪些边缘节点、哪些类型的端设备）。

7.1.2 组建评估团队

团队应包括熟悉系统架构的IT/OT工程师、可靠性工程专家、数据分析师及业务领域专家。明确团队分工与职责。

7.1.3 收集基础资料

包括但不限于：系统架构图、网络拓扑图、设备清单与规格书、软件版本信息、已有的运维规程、历史故障记录与处理报告、相关合同中的SLA条款等。

7.2 数据采集与预处理

7.2.1 数据采集要求

采集不少于连续3个月（对于已运行系统）或基于设计参数的模拟数据（对于新建系统），数据应覆盖正常运行、故障事件、性能波动等场景。

7.2.2 数据预处理

对采集的原始数据进行以下处理：

a）数据清洗：剔除明显错误、重复或无效数据（如心跳包中的异常值）；

b）数据对齐：对不同来源的数据（如设备日志、网络探针数据、应用日志）进行时间戳同步；

c）数据归一化：将不同量纲的指标值转换到同一尺度，便于比较和分析；

d）缺失值处理：采用合理方法（如插值、基于上下文的推断）处理数据缺失；

e）特征提取：从原始数据中提取用于评估模型的特征（如从CPU负载序列中提取平均负载、峰值负载、负载方差等）。

7.3 评估实施步骤

按照以下步骤进行：

a）指标计算：利用预处理后的数据，计算各层级选定的可靠性指标值；

b）模型应用：根据指南选择模型，输入组件可靠性参数（如MTBF、MTTR）或历史数据，进行系统级可靠性计算或预测分析；

c）对比分析：将计算/分析结果与预设的目标值、行业基准或系统历史水平进行对比；

d）薄弱环节识别：找出指标值不达标或显著低于其他同类组件的部分，分析其根本原因（如设计缺陷、配置不当、环境影响、运维不足等）；

e）敏感性分析（可选）：分析关键组件可靠性参数（如MTBF、MTTR）的变化对系统级指标（如A_s）的影响程度，识别最需要改进的环节。

7.4 可靠性等级划分

根据系统可用性（A_s）和关键业务任务成功率（TSR_k）两项核心指标，将流程工业云边端系统的可靠性划分为四个等级，如表8所示。评级时，两项指标应同时满足相应等级要求，若不一致，则以较低等级为准。

表8 流程工业云边端系统可靠性等级

等级	等级名称	系统可用性（A_s）	关键业务任务成功率（TSR_k）	适用场景与要求
1	超高可靠级	≥99.99%	≥99.9%	适用于连续生产、安全联锁、实时优化等对可靠性要求极高的核心系统，要求具备多层次冗余、自动故障切换、异地容灾等能力
2	高可靠级	≥99.95%	≥99.5%	适用于生产监控、先进过程控制（APC）、重要的能源管理等系统，要求具备关键部件冗余和快速恢复机制
3	一般可靠级	≥99.9%	≥99.0%	适用于数据采集与监视（SCADA）、一般性生产报表、视频监控等系统，允许有计划的短暂中断
4	基本可靠级	≥99.5%	≥98.0%	适用于历史数据分析、培训仿真、非关键的管理信息系统等；对业务连续性要求相对宽松

7.5 评估报告编制

评估结束后，应编制正式的可靠性评估报告。报告应内容完整、数据翔实、结论清晰、建议可行。报告至少包括以下章节：

a）报告概述：评估背景、目的、范围、依据、团队及时间；

b）系统描述：详细描述被评估系统的架构、配置和业务功能；

c）评估过程与方法：说明采用的指标体系、数据采集处理过程、评估模型及参数；

d）评估结果与分析：展示各层级指标的详细计算结果，对照目标值或基准进行分析，给出系统最终的可靠性等级评定结果；

e）主要发现与结论：总结系统的整体可靠性水平，明确指出识别出的可靠性薄弱环节、关键风险及其根本原因；

f）改进建议：

——针对设计缺陷，提出架构优化、冗余改进等建议；

——针对运维问题，提出监控加强、巡检规程优化、备件策略调整等建议；

——针对管理问题，提出人员培训、流程完善等建议；

g）附件：包括重要的原始数据摘要、计算过程、模型参数设置、相关图表等。

7.6 报告审批与发布

评估报告完成后，应提交至流程工业企业的相关管理部门进行审批，审批通过后正式发布。评估报告应存档保存，保存期限不少于3年，作为系统后续可靠性管理和技术改造的依据。