ICS 35.240.50
CCS L 67

团　　体　　标　　准

T/CQAE XXXXX—2025

工业操作系统 转型升级水平评估规范

Industrial operating system—Assessment specification of transformation and upgrading level

（报批稿）

2025- XX-XX 发布　　2025- XX-XX 实施

中国电子质量管理协会　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。

本文件由国家工业信息安全发展研究中心提出。

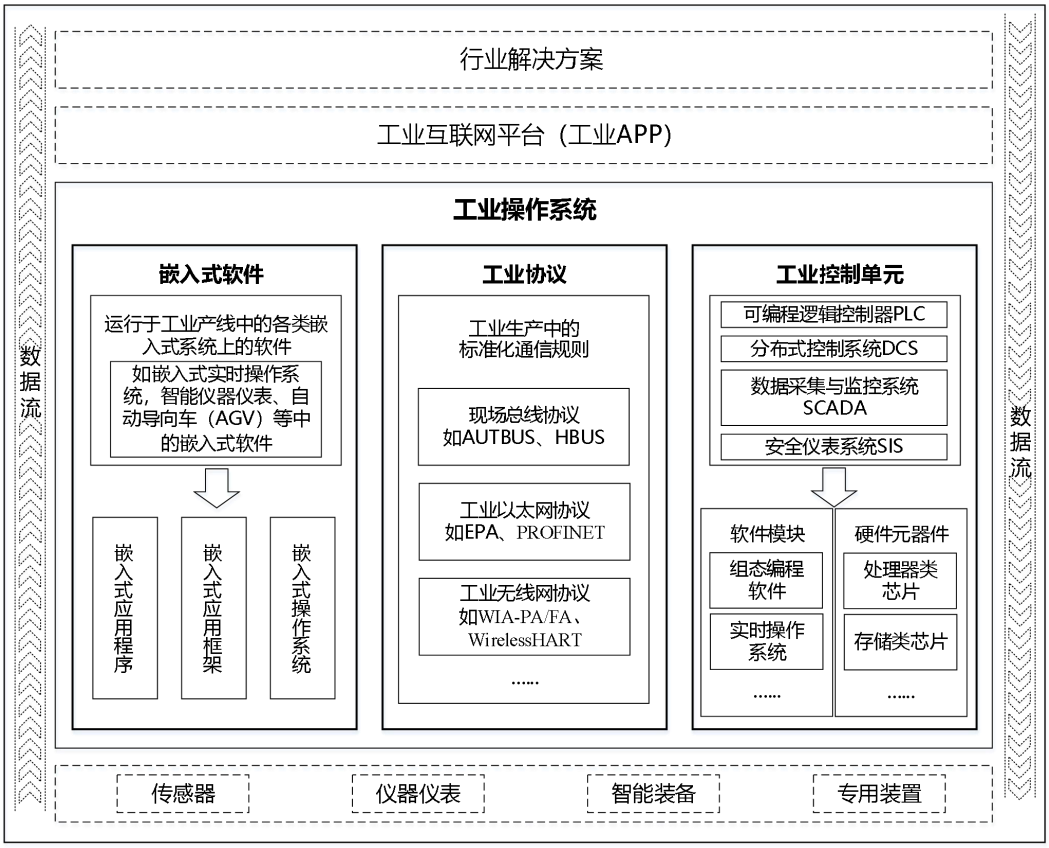
本文件由中国电子质量管理协会归口。

本文件起草单位：国家工业信息安全发展研究中心、工业和信息化部电子第五研究所、中国软件评测中心（工业和信息化部软件与集成电路促进中心）。

本文件主要起草人：孙军、李珣、杨学志、朱笛、李明时、赵阳光、陈平、汤锦依、张慧龑、肖威、翟艳芬、刘亚军。

引言

工业操作系统是实现制造业数字化转型、提升产业链供应链韧性和安全水平的数字底座，主要由嵌入式软件、工业协议和工业控制单元构成，其构成要素及作用关系示意如图1所示，工业操作系统通过数据流，对其下层的传感器、仪器仪表等起到链接作用，对其上层的工业互联网平台、行业解决方案等起到支撑作用，在推进新型工业化中的基础性、支撑性作用日益凸显。



图例：实线部分为工业操作系统内容；虚线部分为其他相关内容。

图1 工业操作系统构成要素及作用关系示意图

随着云计算、大数据、人工智能等新一代信息技术与制造业深度融合，推动工业操作系统转型升级既是支撑制造业数字化转型、实现安全发展的关键举措，也是提升工业操作系统技术、产品和解决方案供给能力的有效路径。

本文件在综合研究分析国际国内相关标准（如IEC 62443、GB/T 20438系列标准等）的基础上，结合工业操作系统技术、产品的应用情况，以及转型升级需求制定，主要目的是：

a）统一对工业操作系统及其转型升级的认识；

b）提供工业操作系统转型升级的方法、路径、典型场景等最佳实践；

c）提供工业操作系统转型升级水平评估内容、指标和方法。

工业操作系统 转型升级水平评估规范

1 范围

本文件提出了工业操作系统转型升级水平的评估对象、内容、指标和方法。

本文件适用于：

a）制造业有关组织（如某行业的集团总部、某个企业或企业内部的某个部门）对生产产线中的工业操作系统转型升级水平开展自评估；

b）工业操作系统提供方对自身的产品或解决方案支撑转型升级水平开展自评估；

c）专业测评机构对制造业有关组织生产产线中的工业操作系统转型升级水平开展独立第三方评估。

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 11457－2006 信息技术 软件工程术语

GB/T 15969.1－2007 可编程程序控制器 第一部分：通用信息

GB/T 50823－2013 油气田及管道工程计算机控制系统设计规范

GB/T 50770－2013 石油化工安全仪表系统设计规范

GB/T 20438.4－2017 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 36637－2018 信息安全技术 ICT供应链安全风险管理指南

GB/T 39477－2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 25069－2022 信息安全技术 术语

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1

操作系统 operating system

指控制各种程序的执行并可提供资源分配、调度、输入输出控制以及数据管理等服务的软件。虽然绝大多数操作系统是软件，部分用固件或硬件实现也是可能的。

[来源：GB/T 11457-2006，2.1055]

3.1.2

工业操作系统 industrial operating system

指能够实时采集、传输、处理工业数据，以及监测生产过程、管理控制单元、保障生产安全的系统。

注：1.结合定义3.1.1，工业操作系统主要包括嵌入式软件（3.1.3）、工业协议（3.1.4）和工业控制单元。

2.工业控制单元包括PLC（3.1.5）、DCS（3.1.6）、SCADA（3.1.7）、SIS（3.1.8）等。

3.1.3

嵌入式软件 embedded software

指运行于生产产线中的各类嵌入式系统上的软件，包括嵌入式应用程序、嵌入式应用框架和嵌入式操作系统。

注：1.如智能仪器仪表、自动导向车（AGV）等中的嵌入式软件。

2.不包括装备中的嵌入式软件。

3.1.4

工业协议 industrial protocol

指工业生产中的标准化通信规则。

3.1.5

可编程逻辑控制器 programmable logic controller

指一种用于工业环境的数字式操作的电子系统。这种系统用可编程的存储器作为面向用户指令的内部寄存器，完成规定的功能，如逻辑、顺序、定时、计数、运算等，通过数字或模拟的输入/输出，控制各种类型的机械或过程。

[来源：GB/T 15969.1-2007，3.5]

3.1.6

分布式控制系统 distributed control system

指一种控制功能分散、操作显示集中、采用分级结构的计算机控制系统，也称为集散控制系统。

[来源：GB/T 50823-2013，2.1.6]

3.1.7

监控和数据采集系统 supervisory control and data acquisition system

指一种以多个远程终端监控单元通过有线或无线网络连接起来，具有远程监测控制功能的分布式计算机控制系统。

[来源：GB/T 50823-2013，2.1.7]

3.1.8

安全仪表系统 safety instrumented system

指一种实现一个或多个安全仪表功能的仪表系统。

[来源：GB/T 50770-2013，2.1.1]

3.1.9

工业外设 peripheral device

指工业操作系统外围的硬件设备，与工业操作系统进行交互，实现输入、输出、存储、通信等功能。

3.1.10

安全完整性等级 safety integrity level

指一种离散的等级（四个可能等级之一），对应安全完整性量值的范围。安全完整性等级4是最高的，安全完整性等级1是最低的。

[来源：GB/T 20438.4-2017，3.5.8]

3.1.11

转型升级水平 transformation and upgrading level

指制造业有关组织生产产线中，工业操作系统应用由被动安全转向以安全可靠为核心的主动安全，并实现提质增效、新技术应用和新模式培育的情况。

3.1.12 **生产产线** production line

指由一系列相互连系的工序和设备按照一定方式排列组成的生产流程，以完成制造产品。

3.1.13 **供应链安全风险** supply chain security risk

供应链安全威胁利用供应链管理中存在的脆弱性导致供应链安全事件的可能性，及其由此对组织造成的影响。

[来源：GB/T 36637-2018，3.5]

3.1.14

规格 specifications

指电子元器件的型号和性能参数，反映元器件功能、性能、封装等一系列关键指标。

3.1.15

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源：GB/T 25069-2022，3.616]

3.1.16

数据安全 data security

采用技术和管理措施来保护数据的保密性、完整性和可用性等。

[来源：GB/T 39477-2020，3.1]

3.1.17

功能安全 function safety

整体安全中与EUC和EUC控制系统相关的部分，它取决于E/E/PE安全相关系统和其他风险降低措施正确执行其功能。

注：1.EUC指受控设备。

2.E/E/PE指电气/电子/可编程电子。

[来源：GB/T 20438.4-2017，3.1.12]

3.2 缩略语

下列缩略语适用于本文件。

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

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

SCADA：监控和数据采集系统（Supervisory Control and Data Acquisition System）

SIL：安全完整性等级（Safety Integrity Level）

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

4 通用要求

4.1 评估对象

评估对象为制造业有关组织新建或在用的，按照评估工作需要选取的某单条生产产线中应用的工业操作系统。对于拥有多条生产产线的集团型或大型企业的评估，需针对不同生产产线进行单独评估并得出对应的评估等级。

4.2 评估内容

4.2.1 供应链安全

供应链安全应评估制造业有关组织生产产线中工业操作系统的安全可靠程度和供应链信息，包括安全可靠和供应链风险防控两部分。具体要求见5.1。

4.2.2 应用安全

应用安全应评估制造业有关组织生产产线中工业操作系统运行和维护过程中采取的安全措施，包括网络安全、数据安全、功能安全三部分。具体要求见5.2。

4.2.3 安全管理能力

安全管理能力应评估制造业有关组织开展工业操作系统建设、开发、运维、升级、改造过程中所遵循的管理规范，包括组织管理、制度建设、人员配备三部分。具体要求见5.3。

4.2.4 转型升级成效

转型升级成效应评估制造业有关组织开展工业操作系统转型升级所带来的经营效果改善和业务流程优化等成效，包括提质增效和新技术应用、新模式培育三部分。具体要求见5.4。

注：本部分评估指标为引导性指标，仅适用于结果为4级的评估对象。

4.3 评估流程

评估流程包括材料提交、资料审核、现场评估、结论出具四个步骤。

a) 材料提交：被评估单位提交材料，包括工业操作系统被评估生产产线的基本情况、工业操作系统产品供应商及产品信息等。

b) 材料审核：评估人员对提交材料的正确性、完整性、真实性审核。

c) 现场评估：评估人员采用访谈、评估等方法，针对生产产线开展工业操作系统转型升级水平评估。

d) 出具结论：评估人员根据资料审核和现场评估的结果，对评估结果进行结论总结，出具评估报告。

4.4 评估等级

为便于识别、改进或提升工业操作系统转型升级水平，应按照表1对评估结果进行由高到低的等级划分。

表 1 工业操作系统转型升级水平评估等级划分表

评估等级	等级描述
4级：引领级	被评估工业操作系统最终得分≥80，其中，供应链安全重要指标得分≥16.6，应用安全重要指标得分≥18.4，安全管理能力重要指标得分≥2.4。
3级：成熟级	被评估工业操作系统最终得分≥70，其中，供应链安全重要指标得分≥14.5，应用安全重要指标得分≥16.1，安全管理能力重要指标得分≥2.1。
2级：改进级	被评估工业操作系统最终得分≥60，其中，供应链安全重要指标得分≥12.5，应用安全重要指标得分≥13.8，安全管理能力重要指标得分≥1.8。
1级：初始级	被评估工业操作系统仅开展转型升级相关规划，但不满足2—4级条件的，划分为本级。

5 评估要求

5.1 供应链安全评估

5.1.1 安全可靠评估

5.1.1.1 嵌入式软件

嵌入式软件安全可靠应评估制造业有关组织生产产线中各类嵌入式系统上的软件应用情况，计算嵌入式软件安全可靠模块的占比。应依据附表A.1开展评估工作。

5.1.1.2 工业协议

工业协议安全可靠应评估制造业有关组织生产产线中工业协议的应用情况，计算安全可靠工业协议应用占比，包括：

a) 安全可靠现场总线协议应用情况。
b) 安全可靠工业以太网协议应用情况。
c) 安全可靠工业无线网协议应用情况。

应依据附表A.2开展评估工作。

5.1.1.3 工业控制单元

工业控制单元安全可靠应评估制造业有关组织生产产线中工业控制单元软硬件的应用情况，按照PLC、DCS、SCADA、SIS的软件模块划分以及芯片与元器件分类，计算工业控制单元安全可靠软件模块占比以及安全可靠芯片与元器件规格占比。应依据附表A.3-A.6开展评估工作。

5.1.1.4 工业外设

工业外设安全可靠应评估制造业有关组织生产产线中工业外设的应用情况，计算安全可靠工业外设占比，包括：

a) 安全可靠输入设备应用情况。
b) 安全可靠输出设备应用情况。
c) 安全可靠存储设备应用情况。
d) 安全可靠通信接口设备应用情况。

应依据附表A.7开展评估工作。

5.1.2 供应链风险防控评估

供应链风险防控应评估制造业有关组织生产产线中工业操作系统供应链全链条安全风险监控和应对的情况。包括：

a) 供应商管理能力：制造业有关组织具备供应链安全规划和管理能力，包括供应链安全管理制度、供应商资质、产品生态情况等。

b) 供应链风险监控：制造业有关组织具备供应链监控及风险识别能力。

c) 供应链风险应对：制造业有关组织具备产品多元化供应及台账跟踪措施，包括备品备件、数字资产台账追溯能力、数字资产台账维护能力。

应依据附表 A.8 开展评估工作。

5.2 应用安全评估

5.2.1 网络安全评估

网络安全应评估制造业有关组织生产产线中工业操作系统运行和维护过程中，采取的网络安全基础和主动防护手段。

基础防护手段包括：

a) 网络构建：设计符合制造业有关组织生产产线实际以及网络安全要求的网络结构。

b) 网络隔离：划分工业生产网络的安全区域。

c) 网络安全评估：评估网络安全风险，包括网络安全风险评估、配置核查。

d) 监测预警：监测制造业有关组织生产产线中工业操作系统的网络安全状态，包括态势感知、威胁预警。

e) 安全防护：采取针对制造业有关组织生产产线中工业生产网络的访问控制、入侵检测、身份鉴别等专用安全策略和技术手段，包括安全防护策略和访问控制。

f) 响应处置：采取针对网络安全事件的手段，包括应急预案与执行、后门及病毒检测、抵御已知威胁。

主动防护手段包括：

g) 协同检测：建立威胁情报共享机制，协同采取风险识别和补救措施。

h) 传输加密：具备完善的网络传输加密机制，保障传输安全。

i) 事件遏制：采取遏制攻击事件的技术手段，包括动态隔离、缩短时间窗口、抵御未知威胁。

j) 溯源干扰：采取针对网络攻击的溯源干扰手段，包括事件溯源、阻断干扰。

应依据附表 B.1 开展评估工作。

5.2.2 数据安全评估

数据安全应评估制造业有关组织生产产线中工业操作系统运行和维护过程中，采取的数据安全基础和主动防护手段。

基础防护手段包括：

a) 资产识别：识别制造业有关组织生产产线中的工业操作系统资产。

b) 数据分离：分离工业生产网络中重要生产产线资产与非重要生产产线资产的数据。

c) 数据安全评估：对生产产线中的工业操作系统数据开展安全评估。

d) 备份恢复：备份重要数据或文件，提高系统恢复能力，包括备份策略、恢复策略、恢复完整性。

主动防护手段包括：

e) 数据加密：使用符合相关国家标准和行业标准的密码技术和产品，保障数据安全。

应依据附表 B.2 开展评估工作。

5.2.3 功能安全评估

功能安全应评估制造业有关组织生产产线针对工业操作系统所采取的可用可靠、配置管理和安全完整性等措施。包括：

a) 可用可靠：采取管理和技术手段，确保系统在规定的运行条件下持续运行，使系统保持可使用状态。

b) 配置管理：实施软件配置管理策略，使软件配置符合最小权限和安全原则，防止未经授权的访问和修改。

c) 安全完整性：采用符合制造业有关组织 SIL 要求的工业操作系统。

应依据附表 B.3 开展评估工作。

5.3 安全管理能力评估

5.3.1 组织管理评估

工业操作系统转型升级工作组织管理应评估：

a) 岗位设置：成立领导小组，实施主要领导负责制，明确管理职责，进行提级管理。

b) 沟通合作：建立跨部门、跨组织协作机制。

c) 条件保障：提供必要的技术、资金、权限等条件保障。

应依据附表C.1开展评估工作。

5.3.2 制度建设评估

工业操作系统转型升级工作制度建设应评估：

a) 方针策略：制定工作专项方针制度，阐明总体目标、范围、原则等。

b) 管理规程：建立管理制度。

c) 审批管理：明确事项审批流程和要求。

d) 制度审定：对制度的合理性和适用性进行论证审定，并定期修订。

应依据附表C.2开展评估工作。

5.3.3 人员配备评估

工业操作系统转型升级工作人员配备应评估：

a) 人员上岗：与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

b) 人员离岗：及时终止离岗人员的访问权限，严格办理调离手续。

c) 人员培训：制定培训计划，开展操作规程、应急处置等培训，定期考核。

应依据附表C.3开展评估工作。

5.4 转型升级成效评估

5.4.1 提质增效评估

提质增效应评估：

a) 降低成本：通过工业操作系统转型升级，降低生产过程中各环节的成本情况。

b) 提高效益：通过工业操作系统转型升级，构建状态感知、实时分析、科学决策、精确执行的管控体系，提高生产效益的情况。

c) 提升质量：通过工业操作系统转型升级，实现生产全过程质量控制和管理，提升产品生产质量和竞争力的情况。

5.4.2 新技术应用评估

新技术应用应评估工业操作系统应用最新的科技成果（人工智能、大数据、云计算、区块链、边缘计算等），提升效率、优化流程、增强产品或服务质量的情况。

5.4.3 新模式培育评估

新模式培育应评估工业操作系统通过技术创新或市场变革，探索和发展新的商业模式、产业模式或管理模式，以适应行业发展趋势的情况。

应依据附表D.1开展评估工作。

6 评估方法

6.1 评估内容的计分方法

工业操作系统转型升级水平评估内容、评估分数与评估指标对应情况如表2所示。

表 2　评估内容、评估分数与评估指标对应表

评估内容			评估指标和方法
5.1供应链安全评估（40分）	5.1.1安全可靠指标（30分）	5.1.1.1嵌入式软件（5分）	附表A.1嵌入式软件安全可靠评估指标和方法表
		5.1.1.2工业协议（3分）	附表A.2工业协议安全可靠评估指标和方法表
		5.1.1.3工业控制单元（20分）	附表A.3-A.6工业控制单元安全可靠评估指标和方法表
		5.1.1.4工业外设（2分）	附表A.7工业外设安全可靠评估指标和方法表
	5.1.2供应链风险防控指标（10分）	/	附表A.8供应链风险防控评估指标和方法表
5.2应用安全评估（40分）	5.2.1网络安全指标（18分）	/	附表B.1网络安全评估指标与评估表
	5.2.2数据安全指标（14分）	/	附表B.2数据安全评估指标和方法表
	5.2.3功能安全指标（8分）	/	附表B.3功能安全评估指标和方法表
5.3安全管理能力评估（10分）	5.3.1组织管理指标（4分）	/	附表C.1组织管理评估指标和方法表
	5.3.2制度建设指标（3分）	/	附表C.2制度建设评估指标和方法表
	5.3.3人员配备指标（3分）	/	附表C.3人员配备评估指标和方法表
5.4转型升级成效评估（10分）	5.4.1提质增效指标（6分）	/	附表D.1转型升级成效评估指标和方法表
	5.4.2新技术应用指标（2分）	/	
	5.4.3新模式培育指标（2分）	/	

6.2　评估结果的计算方法

评估结果应采用累加方式计算，除工业控制单元的安全可靠评估结果按照公式1-公式9计算外，其他评估结果按照附录A-D规定的指标和方法计算：

a）单个工业控制单元安全可靠评估结果应按照公式（1）-（4）进行计算：

$$Q_{PLC}=\frac{\sum(w_{PLC}\times n_{PLC})}{\sum(w_{PLC}\times m_{PLC})} \quad \cdots\cdots (1)$$

$$Q_{DCS}=\frac{\sum(w_{DCS}\times n_{DCS})}{\sum(w_{DCS}\times m_{DCS})} \quad \cdots\cdots (2)$$

$$Q_{SCADA}=\frac{\sum(w_{SCADA}\times n_{SCADA})}{\sum(w_{SCADA}\times m_{SCADA})} \quad \cdots\cdots (3)$$

$$Q_{SIS}=\frac{\sum(w_{SIS}\times n_{SIS})}{\sum(w_{SIS}\times m_{SIS})} \quad \cdots\cdots (4)$$

式中：

Q——单个PLC/DCS/SCADA/SIS安全可靠评估得分；

w——PLC/DCS/SCADA/SIS软件模块/硬件元器件类别权重（对应表A.3-A.6权重一列）；

n——PLC/DCS/SCADA/SIS安全可靠软件模块/硬件元器件数量；

m——PLC/DCS/SCADA/SIS软件模块/硬件元器件数量。

b）各类工业控制单元安全可靠评估结果应按照公式（5）-（8）进行计算：

$$\overline{(Q_{PLC})}=\frac{\sum Q_{PLC}}{X_{PLC}} \quad \cdots\cdots (5)$$

$$\overline{(Q_{DCS})}=\frac{\sum Q_{DCS}}{X_{DCS}} \quad \cdots\cdots (6)$$

$$\overline{(Q_{SCADA})}=\frac{\sum Q_{SCADA}}{X_{SCADA}} \quad \cdots\cdots (7)$$

$$\overline{(Q_{SIS})}=\frac{\sum Q_{SIS}}{X_{SIS}} \quad \cdots\cdots (8)$$

式中：

X——被评估生产产线中PLC/DCS/SCADA/SIS的数量。

c）工业控制单元安全可靠计算公式：

$$S = \frac{\overline{(Q_{PLC})}+\overline{(Q_{DCS})}+\overline{(Q_{SCADA})}+\overline{(Q_{SIS})}}{4} \times 20 \cdots\cdots (9)$$

式中：

S——工业控制单元安全可靠得分。

6.3 评估结果的等级划分

采用累加方式计算工业操作系统转型升级水平总得分，并分别计算供应链安全、应用安全、安全管理能力中重要指标的得分，根据表1确定工业操作系统转型升级水平等级。

附 录 A
（规范性）
供应链安全的评估指标和方法

附录A规定了供应链安全的评估指标和方法，其中：

a） 表A.1规定了嵌入式软件安全可靠的评估指标和方法；
b） 表A.2规定了工业协议安全可靠的评估指标和方法；
c） 表A.3规定了PLC安全可靠的评估指标和方法；
d） 表A.4规定了DCS安全可靠的评估指标和方法；
e） 表A.5规定了SCADA安全可靠的评估指标和方法；
f） 表A.6规定了SIS安全可靠的评估指标和方法；
g） 表A.7规定了工业外设安全可靠的评估指标和方法；
h） 表A.8规定了供应链风险防控的评估指标和方法。

表 A.1 嵌入式软件安全可靠评估指标和方法表

序号	二级指标	三级指标	分值	软件模块类别	评估材料	备注
1	嵌入式软件应用情况	嵌入式应用程序安全可靠情况	2	实时控制、运行操作、数据分析等模块	软件物料清单、需求分析文档、详细设计文档等能够证明嵌入式软件开发、应用的材料	/
2		嵌入式应用程序运行框架安全可靠情况	2	用户界面框架(GUI)、安全管理框架、控制软件框架、容器等模块		/
3		嵌入式操作系统安全可靠情况	3	存储管理、任务管理、中断与异常管理、多指令集架构兼容层、可信根、多核管理、通讯协议、设备驱动、文件系统、接口等模块		重要指标
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。						

表 A.2 工业协议安全可靠评估指标和方法表

序号	二级指标	三级指标	分值	工业协议类别	评估材料	备注
1	工业协议应用情况	现场总线协议应用情况	1	AUTBUS	软件物料清单、需求分析文档、详细设计文档、组态通讯配置文件等能够证明工业协议开发、应用的材料	重要指标
2				HBUS		
3				PROFIBUS DP		
4				Modbus-RTU		
5				CC-Link		
6				DeviceNet		

序号	二级指标	三级指标	分值	工业协议类别	评估材料	备注
7				CANopen		
8				...		
9		工业以太网协议应用情况	1	EPA		重要指标
10				EtherNet/IP		
11				PROFINET		
12				EtherCAT		
13				Modbus-TCP		
14				POWERLINK		
15				...		
16		工业无线网协议应用情况	1	WIA-PA/FA		重要指标
17				WirelessHART		
18				WLAN		
19				Bluetooth		
20				...		
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。						

工业控制单元安全可靠评估根据工业控制单元实际使用的软件模块以及硬件芯片、元器件的类别开展，依据6.2评估方法中的计算公式计算得分情况，工业控制单元安全可靠评估指标与评估方法如表A.3-A.6所示，其中。

$$\text{工业控制单元重要指标得分} = \frac{(PLC\text{安全可靠重要指标得分})+(DCS\text{安全可靠重要指标得分})+(SCADA\text{安全可靠重要指标得分})+(SIS\text{安全可靠重要指标得分})}{(PLC\text{安全可靠得分})+(DCS\text{安全可靠得分})+(SCADA\text{安全可靠得分})+(SIS\text{安全可靠得分})} \times 12.7 \quad \cdots\cdots \quad (10)$$

式中：12.7是按照工业控制单元部分所有重要指标均得分的情况计算而得。

注：除PLC、DCS、SCADA、SIS外，需结合工业控制单元产品形态的适用情况开展评估。

表 A.3 PLC 安全可靠评估指标和方法表

序号	二级指标	类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
1	PLC应用情况	软件	组态编程软件安全可靠情况	5	组态编程软件	软件物料清单、需求分析文档、详细设计文档等能够证明PLC软件开发的材料	重要指标
2			人机界面软件安全可靠情况	3	人机界面（HMI）软件		/
3			控制器软件安全可靠情况	5	运行时系统（固件）		重要指标

序号	二级指标	类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
4			实时操作系统安全可靠情况	5	实时操作系统		重要指标
5		硬件	处理器类芯片安全可靠情况	5	片上系统（SoC）、中央处理器（CPU）、数字信号处理器（DSP）	硬件物料清单	重要指标
6				3	现场可编程逻辑门阵列（FPGA）、复杂可编程逻辑器件（CPLD）、微控制单元（MCU）	硬件物料清单	/
7			存储类芯片安全可靠情况	3	双倍速率同步动态随机存储器（DDR）、静态随机存取存储器（SRAM）	硬件物料清单	/
8				1	NOR型闪存（NORFLASH）、NAND闪存（NANDFLASH）、内嵌式存储器标准规格（eMMC）芯片、非易失性的磁性随机存储器（MRAM）芯片	硬件物料清单	/
9			模拟类芯片安全可靠情况	5	模数/数模转换器（ADC/DAC）芯片品牌	硬件物料清单	重要指标
10				3	电压基准源、驱动芯片	硬件物料清单	/
11				1	运放、比较器、传感器芯片	硬件物料清单	/
12			通信接口类芯片安全可靠情况	3	低电压差分信号（LVDS）、工业以太网、工业总线、无源射频	硬件物料清单	/
13				1	EIA-RS485串行通信接口、EIA-RS232串行通信接口芯片	硬件物料清单	/
14			电源管理类芯片安全可靠情况	1	线性电源、电源控制、电流检测、电源监视、看门狗芯片	硬件物料清单	/
15			晶振和时钟元器件安全可靠情况	3	晶振、时钟芯片	硬件物料清单	/
16				1	时钟缓冲器	硬件物料清单	/

注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。
2.不适用项，按照得分计算。

表 A.4 DCS 安全可靠评估指标和方法表

序号	二级指标	工业控制单元类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
1	DCS应用情况	软件	组态编程软件安全可靠情况	5	组态编程软件	软件物料清单、需求分析文档、详细设计文档等能够证明DCS软件开发的材料	重要指标
2			监控软件安全可靠情况	5	监控软件		重要指标
3			人机界面软件安全可靠情况	3	人机界面（HMI）软件		/
4			应用程序安全可靠情况	5	实时控制软件、报警与事件管理软件、报表和数据分析工具、设备管理软件等		重要指标
5			数据库安全可靠情况	5	实时数据库、历史数据库、关系型数据库		重要指标
8			控制器软件安全可靠情况	5	运行时系统（固件）		重要指标
9			实时操作系统安全可靠情况	5	实时操作系统		重要指标
10		硬件	处理器类芯片安全可靠情况	5	片上系统（SoC）、中央处理器（CPU）、数字信号处理器（DSP）	硬件物料清单	重要指标
11				3	现场可编程逻辑门阵列（FPGA）、复杂可编程逻辑器件（CPLD）、微控制单元（MCU）	硬件物料清单	/
12			存储类芯片安全可靠情况	3	双倍速率同步动态随机存储器（DDR）、静态随机存取存储器（SRAM）	硬件物料清单	/
13				1	NOR型闪存（NORFLASH）、NAND闪存（NANDFLASH）、内嵌式存储器标准规格（eMMC）芯片、非易失性的磁性随机存储器（MRAM）芯片	硬件物料清单	/
14			模拟类芯片安全可靠情况	5	模数/数模转换器（ADC/DAC）芯片品牌	硬件物料清单	重要指标
15				3	电压基准源、驱动芯片	硬件物料清单	/
16				1	运放、比较器、传感器芯片	硬件物料清单	/
17			通信接口类芯片安全可靠情况	3	低电压差分信号（LVDS）、工业以太网、工业总线、无源射频	硬件物料清单	/
18				1	EIA-RS485串行通信接口、EIA-RS232串行通信接口芯片	硬件物料清单	/
19			电源管理类芯片安全	1	线性电源、电源控制、电流检测、电源监视、	硬件物料清单	/

序号	二级指标	工业控制单元类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
			可靠情况		看门狗芯片		
20			晶振和时钟元器件安全可靠情况	3	晶振、时钟芯片	硬件物料清单	/
21				1	时钟缓冲器	硬件物料清单	/
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。							

表 A.5 SCADA 安全可靠评估指标和方法表

序号	二级指标	工业控制单元类型	三级指标	权重（对应公式1-4中的w）	软件模块类别	评估材料	备注
1	SCADA应用情况	软件	组态编程软件安全可靠情况	5	组态编程软件	软件物料清单、需求分析文档、详细设计文档等能够证明SCADA软件开发的材料	重要指标
2			监控软件安全可靠情况	5	监控软件		重要指标
3			应用程序安全可靠情况	5	生产过程可视化软件		重要指标
4			数据库安全可靠情况	5	实时数据库、历史数据库、关系型数据库		重要指标
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。							

表 A.6 SIS 安全可靠评估指标和方法表

序号	二级指标	工业控制单元类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
1	SIS应用情况	软件	组态编程软件安全可靠情况	5	安全组态软件	软件物料清单、需求分析文档、详细设计文档等能够证明SIS软件开发的材料	重要指标
2			应用程序安全可靠情况	5	应用程序		重要指标
3			控制器软件安全可靠情况	5	运行时系统（固件）		重要指标
4			实时操作系统安全可靠情况	5	实时操作系统		重要指标

序号	二级指标	工业控制单元类型	三级指标	权重（对应公式1-4中的w）	软件模块/硬件元器件类别	评估材料	备注
5			处理器类芯片安全可靠情况	5	片上系统（SoC）、中央处理器（CPU）、数字信号处理器（DSP）	硬件物料清单	重要指标
6				3	现场可编程逻辑门阵列（FPGA）、复杂可编程逻辑器件（CPLD）、微控制单元（MCU）	硬件物料清单	/
7			存储类芯片安全可靠情况	3	双倍速率同步动态随机存储器（DDR）、静态随机存取存储器（SRAM）	硬件物料清单	/
8				1	NOR型闪存（NORFLASH）、NAND闪存（NANDFLASH）、内嵌式存储器标准规格（eMMC）芯片、非易失性的磁性随机存储器（MRAM）芯片	硬件物料清单	/
9			模拟类芯片安全可靠情况	5	模数/数模转换器（ADC/DAC）芯片品牌	硬件物料清单	重要指标
10				3	电压基准源、驱动芯片	硬件物料清单	/
11		硬件		1	运放、比较器、传感器芯片	硬件物料清单	/
12			通信接口类芯片安全可靠情况	3	低电压差分信号（LVDS）、工业以太网、工业总线、无源射频	硬件物料清单	/
13				1	EIA-RS485串行通信接口、EIA-RS232串行通信接口芯片	硬件物料清单	/
14			电源管理类芯片安全可靠情况	1	线性电源、电源控制、电流检测、电源监视、看门狗芯片	硬件物料清单	/
15			晶振和时钟元器件安全可靠情况	3	晶振、时钟芯片	硬件物料清单	/
16				1	时钟缓冲器	硬件物料清单	/

注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。
2.不适用项，按照得分计算。

表 A.7 工业外设安全可靠评估指标和方法表

序号	二级指标	三级指标	分值	工业外设类别	评估材料	备注
1	工业外设安全可靠情况	输入设备安全可靠情况	0.5	键盘、触摸屏、语音输入设备、按键管理、触摸输入设备、输入信号抗干扰、按键去抖动等设备和模块	设备物料清单、需求分析文档、详细设计文档等能够证明工业外设研制、应用的材料	重要指标
2		输出设备安全可靠情况	0.5	摄像头、显示屏、指示灯、蜂鸣器、亮度响度控制等设备和模块		重要指标
3		存储设备安全可靠情况	0.5	外部存储设备、安全擦除、读写异常恢复、数据完整性校验等设备和模块		重要指标
4		通信接口设备安全可靠情况	0.5	通用串行总线（USB）、通用串行数据总线（UART）、串行外设接口（SPI）、双向二线制同步串行总线（I2C）、无线保真技术（Wireless Fidelity）、近场通信（NFC）等设备和模块		重要指标
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。						

表 A.8 供应链风险防控评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	供应商管理能力	供应链安全管理制度	1	供应链安全管理制度情况	供应链安全策略及应对措施等	/
		供应商资质	0.5	供应商安全生产资质情况	供应商安全生产资质证书等	/
		产品生态情况	0.5	安全可靠品牌芯片和安全可靠品牌通用操	安全可靠品牌芯片及安全可靠品牌通用操作	/

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
				作系统兼容情况	系统适配/兼容报告等相关证明文件	
		服务保障体系	0.5	服务保障协议情况	售后服务体系以及相关协议文件等	/
		供应商选取	0.5	供应商遴选情况	供应商管理制度等相关文档	/
			1	供应商目录管理情况	供应商目录及更新情况	/
2	供应链风险监控	供应链监控	1	供应链信息掌握情况	供应链监测系统或供应链稳定性分析报告	/
		供应链风险识别	1	供应链威胁风险识别情况	供应链风险识别、应对方案等	重要指标
3	供应链风险应对	备品备件	3	国外品牌产品备件情况	备品备件系统或库存管理等相关文档	/
				国内品牌产品备件情况		
				国内外产品供应中断应对情况	供应中断应对方案、产品试用等相关文档	重要指标
		数字资产台账追溯能力	0.5	供应商追溯情况	供应商溯源登记表，如：物料清单、数字资产台账清单，记录供应链所有实体要素，包括软件、硬件来源等	/
		数字资产台账维护能力	0.5	数字资产台账维护情况	数字资产台账更新记录，产品/系统使用、检测和维护记录等	/

注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。
2.不适用项，按照得分计算。

附 录 B
（规范性）
应用安全的评估指标和方法

附录B规定了应用安全的评估指标和方法，其中：

a） 表B.1规定了网络安全的评估指标和方法；

b） 表B.2规定了数据安全的评估指标和方法；

c） 表B.3规定了功能安全的评估指标和方法。

表 B.1 网络安全的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	网络构建	网络节点地理分布及网络架构设计	1	网络设备、网络线路安全情况	网络拓扑图、等保定级检测记录等	/
2	网络隔离	网络分段或分区管理	1	基于重要生产产线的网络进行分段或分区管理情况	网络拓扑图、等保定级检测记录等	/
3	网络安全评估	网络安全风险评估	1.5	网络安全评估情况	代码静动态安全审计报告、代码功能测试报告、网络安全风险评估报告	重要指标
		配置核查	1.5	网络安全设备配置及运行情况	安全设置要求、安全巡检记录等	重要指标
4	监测预警	态势感知	1.5	网络安全监测情况	查看态势感知系统部署和应用情况	重要指标
		威胁预警	0.5	威胁发现及预警情况	安全威胁发现和处理系统、处理记录文档等	/
5	安全防护	安全防护策略	1.5	工业生产网络专用防护情况	查看工业生产网络内部部署的安全设备或防护措施，如IPS、IDS、数据库审计、日志审计、远程访问控制等安全设备	重要指标
		访问控制	1	访问权限管控情况	访问控制策略文件、审计记录	/
6	响应处置	应急预案与执行	1.5	应急预案及应急演练情况	应急预案管理制度文件、应急预案、应急演练记录等	重要指标
			0.5	应急预案更新情况	应急预案修订、评审、培训记录等	/
		后门及病毒检测	0.5	软硬件后门检测情况	软硬件后门、病毒检测记录等	/
			0.5	漏洞库升级情况	病毒库升级记录	/
			0.5	病毒扫描情况	病毒扫描记录	/
		抵御已知威胁	0.5	已知特征的网络攻击抵御情况	查看漏洞修复、网络攻击特征升级手段	/
7	协同检测	情报共享	0.5	威胁情报获取情况	查看情报共享的方式，例如威胁情报共享平台或威胁情报库列表	/

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
8	传输加密	网络传输加密	1	网络传输加密情况	密码设备使用要求、招标要求或密码设备使用说明等	重要指标
9	事件遏制	动态隔离	1	针对动态隔离的措施情况	应急预案、应急演练记录等	重要指标
		缩短时间窗口	0.5	缩短安全事件时间的能力情况	技术文档或应急预案等	/
		抵御未知威胁	0.5	未知特征的网络攻击抵御情况	黑白名单控制手段、异常流量发现、日志审计等手段	/
10	溯源干扰	事件溯源	0.5	网络攻击溯源分析情况	互联网协议地址（IP）地址追踪、域名追溯、数据包分析和时间线重建等技术手段	/
		阻断干扰	0.5	网络攻击干扰阻断情况	阻断干扰网络攻击的技术手段	/
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。						

表 B.2 数据安全的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	资产识别	识别业务资产	2	工业操作系统资产掌握情况	业务清单、工业操作系统资产清单	重要指标
2	数据分离	资产分离保护	1.5	重要生产产线资产与非重要生产产线资产的分离情况	业务清单、网络、设备隔离技术文档或应急演练记录等	/
3	数据安全评估	数据安全风险评估	3	数据安全评估情况	数据安全风险评估报告	重要指标
4	备份恢复	备份策略	2	备份执行情况	备份与恢复软件、备份管理制度文件、备份记录等	重要指标
			1	异地备份情况	异地备份相关设计、执行、演练文档等	/
		恢复策略	1	恢复策略情况	多节点备份相关设计、执行、演练文档等	/
		恢复完整性	1.5	备份恢复完整性情况	系统测试报告、应急预案、应急演练记录等	/
5	数据加密	设备加密使用	2	设备加密使用情况	招标要求、密码设备使用要求、密码设备使用说明等	/
注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。 2.不适用项，按照得分计算。						

表 B.3 功能安全的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	可用可靠	可用可靠能力	1.5	可用可靠情况	运行记录等	重要指标
		容错能力	0.5	系统鲁棒性和系统容错方法情况	测试报告、应急预案、应急演练记录等	/
		业务切换	0.5	针对业务系统切换的措施情况	应急预案、应急演练记录等	/
		重续运行	0.5	针对灾备、多节点业务的措施情况	应急预案、应急演练记录等	/
2	配置管理	软件更新渠道及软件完整性	0.5	软件更新情况	软件更新与变更管理制度等	重要指标
		更新及时性	0.5	软件更新机制情况	软件更新与变更管理制度、软件更新记录等	重要指标
		回滚机制	0.5	软件回滚机制情况	软件更新及回滚计划等	/
		更新授权和验证机制	0.5	软件更新授权机制	软件更新授权和审计记录等	/
		最小服务和功能启用	0.5	软件最小化服务情况	软件安装说明、软件配置管理方案、软件配置记录等	/
		密码策略	0.5	软件密码策略情况	软件配置管理方案等	/
3	安全完整性	标准符合性	1	符合功能安全标准中整体安全生命周期要求的情况	安全要求规格书、系统级危险分析和风险评估报告等	重要指标
		SIL	1	SIL情况	SIS适用。SIL评定结果等	重要指标

注：1.现场条件不允许的情况下，可采信供应商提供的第三方测试报告或认证证书。
2.不适用项，按照得分计算。

附 录 C
（规范性）
安全管理能力的评估指标和方法

附录C规定了安全管理能力的评估指标和方法，其中：

a） 表C.1规定了组织管理的评估指标和方法；

b） 表C.2规定了制度建设的评估指标和方法；

c） 表C.3规定了人员配备的评估指标和方法。

表 C.1 组织管理的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	组织管理	岗位设置	2	机构设置情况	机构设置、岗位设置文件等	/
				负责人设置情况	人员职责文档等	重要指标
		沟通合作	1	沟通合作情况	会议记录、专家库、外联表等	/
		条件保障	1	条件保障情况	条件保障文件，如预算报告、可行性分析报告、人员职责文件等	/

表 C.2 制度建设的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	制度建设	方针策略	1	方针政策制定情况	总体方针、策略制度等	重要指标
		管理规程	1	管理制度情况	安全管理制度、操作规程、安全管理制度等	/
				技术管理制度情况	技术方案评审、运维制度等	
		审批管理	0.5	审批制度情况	审批制度、审批记录等	/
		制度审定	0.5	制度制定、论证情况	制度论证、评审记录等	/
				制度修订情况	制度修订记录等	

表 C.3 人员配备的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	人员配备	人员上岗	1	协议制定情况	人员上岗管理文档、上岗审查记录、岗位责任协议等	/
		人员离岗	0.5	离岗管理制定情况	人员离岗制度等	/
				离岗手续执行情况	人员离岗记录等	
		人员培训	1.5	培训考核制度制定情况	培训制度、培训计划、考核计划等	/
				培训考核制度执行情况	培训记录、考核记录等	重要指标

附 录 D
（规范性）
转型升级成效的评估指标和方法

附录D.1规定了转型升级成效的评估指标和方法。

表 D.1 转型升级成效的评估指标和方法表

序号	二级指标	三级指标	分值	评估要求	评估材料	备注
1	提质增效	降低成本	2	成本降低情况	重点生产环节和生产场景成本财务记录，工业操作系统相关改造设计与研发文档等	/
		提高效益	2	生产效益提高情况	工厂生产管控体系建设、管理相关报告，生产环节绿色节能相关报告，工业操作系统相关改造设计与研发文档等	/
		提升质量	2	生产质量提升情况	生产质量控制记录、良品率数据改善相关记录、工业操作系统相关改造设计与研发文档等	/
2	新技术应用	技术创新	2	新技术应用情况	工业操作系统设计与研发文档；改造计划或实施方案文档等	/
3	新模式培育	模式创新	2	新模式培育情况	全量数据采集记录；生产产线有关生产运行记录；生产产线设计、改造计划、说明文档或操作手册等	/

参考文献

[1]GB/T 28827.3－2012 信息技术服务 运行维护 第3部分：应急响应规范
[2]GB/T 30146－2013/ISO 22301: 2012 业务连续性管理体系
[3]GB/T 20438.1－2017 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
[4]GB/T 20438.2－2017 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
[5]GB/T 20438.3－2017 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
[6]GB/T 35320－2017 危险与可操作性分析（HAZOP分析）应用指南
[7]GB/T 20984－2022 网络与数据安全技术 网络与数据安全风险评估方法
[8]GB/T 39204－2022 网络与数据安全技术 关键信息基础设施安全保护要求
[9]GB/T 44862－2024 网络安全技术 网络弹性评价准则