|  |  |
| --- | --- |
| ICS | 35.030 |
| CCS | M10 |

中华人民共和国国家标准

GB/T XXXXX—XXXX



工业互联网企业网络安全：第一部分 应用工业互联网的工业企业防护要求

Industrial Internet enterprise network security: Part I Baseline for cybersecurity protection of Internet Industrial Enterprise

(点击此处添加与国际标准一致性程度的标识)

（完成时间：2022-08-20）

XXXX - XX - XX发布

XXXX - XX - XX实施



目次

[1 范围 1](#_Toc5141)

[2 规范性引用文件 1](#_Toc21618)

[3 术语和定义 1](#_Toc2079)

[4 缩略语 1](#_Toc5882)

[5 应用工业互联网的工业企业网络安全防护内容 2](#_Toc5169)

[6 应用工业互联网的工业企业网络安全防护级别的确定 2](#_Toc26856)

[7 应用工业互联网的工业企业网络安全防护要求 2](#_Toc26783)

1. 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。

本文件由全国通信标准化技术委员会（SAC/TC485）归口。

本文件起草单位：XXX

本文件主要起草人：XXX

工业互联网企业网络安全：第一部分 应用工业互联网的工业企业防护要求

* 1. 范围

本文件给出了应用工业互联网的工业企业网络安全防护需达到的具体级别和相应的防护要求。

本文件适用于应用工业互联网的工业企业开展网络安全防护情况评估或自评估。应用工业互联网的工业企业网络安全防护范围包括依托于工业互联网服务的各类信息系统、控制系统、应用等安全以及企业整体网络安全管理。

* 1. 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 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

GB 50174—2017 数据中心设计规范

GB/Z 41288—2022 信息安全技术 重要工业控制系统网络安全防护导则

GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型

GB/T XXXXX—XXXX 工业互联网企业网络安全 第2部分：平台企业防护要求

GB/T XXXXX—XXXX 工业互联网企业网络安全 第4部分：数据防护要求

YD/T 1754—2008 电信网和互联网物理环境安全等级保护要求

XXXX-XXXX 应用工业互联网的工业企业定级规则

* 1. 术语和定义

GB/T 25069、GB/T 32919-2016界定的以及下列术语和定义适用于本文件。

工业互联网 Industrial Internet

工业互联网是新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系，为工业乃至产业数字化、网络化、智能化发展提供了实现途径。

应用工业互联网的工业企业 Internet Industrial Enterprise

运用工业互联网技术实现智能控制、运营优化和生产组织方式的工业企业。

* 1. 缩略语

下列缩略语适用于本文件。

AGV：自动导引运输车（Automated Guided Vehicle）

CNC：计算机数字控制机床（Computer numerical control）

APP：应用程序（Application）加速并行处理技术（Accelerated Parallel Processing）

RTU：远程测控终端，远程终端单元（Remote Terminal Unit）

IED：智能电子设备（Intelligent Electronic Device）

DPU：分散处理单元(Distributed Processing Unit)

* 1. 应用工业互联网的工业企业网络安全防护内容

应用工业互联网的工业企业网络安全防护内容具体包括：

（1）设备安全防护：包括工业主机安全、网络设备安全、工业控制设备安全等。

（2）控制安全防护：包括应用工业互联网的工业企业控制系统安全、组态软件安全、配置安全、智能装备控制安全等。

（3）网络安全防护：包括架构安全、边界安全、通信安全等。

（4）数据安全防护：参照《工业互联网企业网络安全 第4部分：数据防护要求》。

（5）软件安全防护：包括生产控制软件、本地部署平台软件、第三方平台软件、工业APP等。

（6）网络安全管理要求：包括安全管理制度、安全管理机构和人员、安全建设管理、安全运维管理等。

（7）物理和环境安全要求：包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等。

* 1. 应用工业互联网的工业企业网络安全防护级别的确定

应用工业互联网的工业企业按照《应用工业互联网的工业企业定级规则》划分级别，采取不同程度的安全防护。应用工业互联网的工业企业的安全防护要求分为基本级和增强级两个级别，其中：

三级的应用工业互联网的工业企业按照增强级防护要求采取防护措施；

二级的应用工业互联网的工业企业按照基本级防护要求采取防护措施；

一级的应用工业互联网的工业企业根据自身情况参照基本级防护要求，自主落实安全防护措施。

* 1. 应用工业互联网的工业企业网络安全防护要求
     1. 基本级防护要求
        1. 设备安全防护要求
           1. 工业主机安全防护要求

1. 应对主机设备的账户和口令进行管理，合理设置账户类型和权限，使用强口令并保持定期更换；
2. 应配置主机设备安全策略，并建立安全策略配置清单，定期确认相关安全策略的合规性和有效性；
3. 应对移动存储介质的接入和使用的权限进行管理和控制；
4. 应对工业主机系统上软件程序的安装、卸载和运行进行管理和控制；
5. 应对工业主机外部接口进行管控，对外部接入设备，特别是有线或无线通信设备进行管理和控制；
6. 应关闭与系统业务无关的端口和服务；
7. 应规范软硬件安装和使用，不应在未授权的情况下擅自安装、卸载、升级软件，擅自更改软硬件配置。
   * + - 1. 网络设备安全防护要求
8. 应对网络设备上账户、口令等内容进行检查，严禁使用空口令、弱口令，及时处理多余、过期、共享、僵尸账户；
9. 应对网络设备的运行日志和操作日志进行定期审计分析，发现安全风险或问题，应及时处理；
10. 应对网络设备的远程维护实行实时监管和审计，防止高危操作影响正常业务运行；
11. 应对网络设备的接口进行管控，关闭或封锁不使用的网络端口；
12. 应加强对无线设备接入无线通信网络设备的访问管控，防止未认证设备的接入访问；
13. 应定期对网络设备的业务配置和安全配置进行核查，防止网络安全风险的发生影响业务系统；
14. 网络关键设备和网络安全专用产品应符合相关国家标准的强制性要求。
    * + - 1. 工业控制设备安全防护要求
15. 工业控制设备自身应实现对于用户登录访问的身份鉴别的安全要求；
16. 工业控制设备自身应实现对于重要的用户行为和重要安全事件进行安全审计；
17. 对采用无线通信技术进行控制的工业控制设备，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为；
18. 对采用无线通信技术进行控制的工业控制设备，应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；
19. 如受条件限制控制设备无法采用上述身份鉴别措施，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
20. 选择现场测控设备应优先考虑具有对访问行为主体（人员、进程和设备）进行标识与鉴别的功能；
21. 选择现场测控设备应优先考虑具有访问控制与审计功能，支持基于角色的访问控制策略，并对重要的安全性事件和重要生产活动进行审计；
22. 选择现场测控设备应优先考虑具有数据完整性校验功能，具备防止对静态数据进行非授权写操作的保护机制（硬件或软件），并具备抵御数据包插入、丢失、重放、篡改的机制；
23. 采用的现场测控设备应具备保护存储和传输数据保密性的机制。
    * + 1. 控制安全防护要求
           1. 应用工业互联网的工业企业控制系统安全防护要求
24. 应建立工业控制系统的入侵防范管理机制；
25. 应对工业控制系统进行用户登录认证管理和权限控制；
26. 应对重要工业控制系统部署访问控制、操作审计等安全措施；
27. 应每半年针对工业主机进行一次恶意代码查杀，对临时接入设备在接入前进行恶意代码查杀，并留存相应记录；
28. 应对配置安全策略进行定期评估优化，并建立安全策略配置清单；
29. 工业控制系统不应与互联网直接相连，如确需连接互联网并从工业控制系统获取数据时，应部署单向隔离装置进行防护，以防止外部对工业控制系统进行渗透攻击和控制操作；
30. 应对工业控制系统相关访问日志（包括人员账户、访问时间、操作、内容等）保留至少6个月，并定期备份防止丢失或被篡改；
31. 对于新部署的工业控制系统，应在上线前进行安全检查评估。
    * + - 1. 组态软件安全要求
32. 应对组态软件进行用户登录认证管理和权限控制；
33. 应对组态软件应用层代码文件、工程文件、操作记录文件等进行完整性保护；
34. 应对组态软件的通信进行完整性保护；
35. 应具备对组态软件登录、访问、操作等审计措施；
36. 对新部署组态软件，应在上线前进行安全检查评估。
    * + - 1. 配置安全要求
37. 应建立针对控制服务器等重要工业控制系统关键设备安全配置的备份和审计机制，审计记录应至少包含访问控制、配置变更操作、配置变更结果及时间戳等信息
38. 应按照最小化原则禁用非必要的后台程序、进程、端口、服务，应定期对账户、口令、端口、服务等内容进行检查，及时处理多余、过期、共享、僵尸账户；
39. 在进行配置变更时，应先完成配置变更测试验证，验证之后方可进行正式的配置变更，应对变更操作进行记录，在出现配置变更问题时可以进行快速回退复原；
40. 任何配置变更，应得到批准才能执行；紧急情况的变更，按照约定的程序执行；
    * + - 1. 智能装备控制安全要求
41. 对工业互联网平台直接控制的现场重要设备（如AGV、工业机器人、CNC数控机床、工业网关等），应确认设备身份的唯一性安全标识，以便针对现场重要设备进行安全识别和访问控制；
42. 现场重要设备应具有基本的对控制指令的来源识别验证、访问控制功能；
43. 应采用校验技术或密码技术，使现场重要设备在进行数据交互过程中实现数据的完整性校验和机密性传输。
    * + 1. 网络安全防护要求
           1. 架构安全要求
44. 在工业企业网络安全架构的设计、开发和更改前应考虑潜在的安全风险和所承载业务的重要性，实施并通过安全检查评估，并定期（例如每年）对网络安全架构进行评审；
45. 应根据安全风险评估结果，对工业企业划分不同的网络安全域，并按照方便管理和控制的原则为各安全域分配地址；
46. 应将控制系统网络与非控制系统网络进行逻辑分区，将关键控制系统网络与非关键控制系统网络进行逻辑分区；
47. 工业企业的网络带宽设计指标应大于网络带宽需求指标，网络带宽的大小应满足业务高峰期需求，并考虑异常生产工况、突发业务等情况下的带宽需求；
48. 应保证网络设备的业务处理能力满足业务高峰期需要；
    * + - 1. 边界安全要求
49. 工业企业应定义明确企业网络与互联网、企业网络内部各控制系统网络和非控制系统网络、关键控制系统网络与非关键控制系统网络的安全边界；
50. 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
51. 应对与互联网及其他公共信息网络进行逻辑隔离；
52. 应在控制系统或工业控制现场设备和互联网的边界采取安全防护措施；
53. 应对网络边界进行安全监测，识别网络边界的入侵行为；
54. 应能对网络边界的入侵行为进行有效阻断；
    * + - 1. 通信安全要求
55. 应采用校验码技术或加解密技术保证工业企业网络通信传输的完整性；
56. 应采用加解密技术保证工业企业网络通信传输的保密性；
57. 通过互联网及其他公共信息网络进行通信数据传输时，应采用加密认证技术手段进行数据传输，对传输设备进行身份认证、访问控制；
58. 应对无线连接的授权、监视以及执行使用进行限制；
    * + 1. 数据安全防护要求

应按照《工业互联网企业网络安全 第4部分：数据防护要求》对应用工业互联网的工业企业所使用的数据进行分类分级，依据分级要求采取对应的数据安全防护措施。

* + - 1. 软件安全防护要求
         1. 工业互联网设备固件安全要求

1. 应建立各类工业互联网设备的设备型号、固件名称、固件版本及固件系统信息等安全台账信息；
2. 依据安全台账信息，应定期检查工业互联网安全漏洞平台披露的漏洞信息，如检查发现存在高危漏洞设备，应第一时间启动应急处置并联系厂商升级固件；
3. 设备固件升级前应确认固件文件的特征码与厂商提供的特征码一致，避免固件被恶意篡改或替换；
4. 设备固件升级应具有向后兼容性，固件升级后系统应保留原有的配置信息；
5. 设备固件升级前应利用固件安全检测工具静态扫描漏洞后门，提前发现越权执行、缓冲区溢出、远程命令执行、密钥泄露、隐藏后门、配置不当等各种安全隐患。
   * + - 1. 生产控制软件安全要求
6. 生产控制软件开发、升级或更新后，应进行充分的离线测试，确保软件的可用性和安全性后，再部署到工业企业现场；
7. 应具备登录控制功能，对登录用户进行身份识别和鉴别；
8. 应保存启动、停止、复位以及用户登录、退出等关键动作的操作日志，并定期审计；
9. 如果生产控制软件本身无法实现安全要求，可以通过网络设备、安全设备或安全管理等其他设备或手段，满足相应的安全要求。
   * + - 1. 本地部署平台软件安全要求
10. 平台软件开发、升级或更新后，应进行充分的测试，确保软件的可用性和安全性后，再部署到工业企业现场；
11. 应建立统一的安全机制，包括安全事件识别、响应、报送、处置机制；
12. 应在平台内部区分不同模块的读写权限并限制读写范围；
13. 应具备虚拟化安全设备，对平台内的功能模块、虚拟机等资源进行安全防护。
    * + - 1. 第三方平台软件安全要求
14. 第三方平台软件开发、升级或更新后，应进行充分的测试，确保软件的可用性和安全性后，再部署到工业企业现场；
15. 在使用第三方平台的过程中，应定期更新平台软件，确保及时消除平台漏洞和隐患；
16. 应明确区分工业企业与第三方平台的管理边界，工业企业应保存所管理软件的操作日志，并定期审计；
17. 应限制接口的访问权限，并验证接口调用程序的电子签名，或采用其他方式确认调用程序的合法性；
18. 应按照分级分类原则，管理接入第三方云平台软件的企业数据。
    * + - 1. 工业APP安全要求
19. 工业APP开发、升级或更新后，应进行充分的测试，确保软件的可用性和安全性后，再部署到工业企业现场；
20. 应在工业APP中集成具有网络安全防护功能的模块；
21. 应对使用工业APP的用户进行身份认证；
22. 在使用工业APP过程中，应当区分工程师、操作员、管理员、审计员等不同角色，并赋予不同操作权限。
    * + 1. 网络安全管理要求
           1. 安全管理制度
23. 应对安全管理活动中重要的管理内容建立安全管理制度；
24. 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
25. 应指定或授权专门的部门或人员负责安全管理制度的制定；
26. 安全管理制度应通过正式、有效的方式发布，并进行版本控制；
27. 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
    * + - 1. 安全管理机构和人员要求

安全管理机构

1. 应明确指定特定机构，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，实施网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；
2. 应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并明确部门及各负责人的职责；
3. 应设立系统管理员、网络管理员、安全管理员等岗位，配备一定数量的系统管理员、网络管理员、安全管理员等，并明确各个工作岗位的职责；
4. 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
5. 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。

人员要求

1. 应加强各类管理人员之间、组织内部机构之间以及安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理安全问题；
2. 应加强与工业互联网安全主管部门、各类供应商、业界专家等合作与沟通；
3. 应指定或授权特定的部门或人员负责人员录用；
4. 应对被录用人员的身份、背景、专业资格和资质等进行审查；
5. 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
6. 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
7. 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
8. 外部人员离场后应及时清除其所有的访问权限。
   * + - 1. 安全建设管理要求

定级

1. 应按照《应用工业互联网的工业企业定级规则》明确本企业的安全等级；
2. 应以书面形式说明企业确定为某安全等级的方法和理由。

安全方案设计

1. 应根据安全防护对象的安全防护需求进行安全方案设计；
2. 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用

1. 工业控制系统、工业互联网平台或标识解析系统的重要设备及专用安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
2. 应确保安全产品与服务的采购和使用符合国家的有关规定。

软件开发

1. 应确保开发环境与实际运行环境物理隔离，测试数据和测试结果受到控制；
2. 应在软件开发过程中进行安全性测试；
3. 应在软件交付前检测其中可能存在的缺陷与恶意代码等；
4. 应要求开发单位提供软件设计文档和使用指南；
5. 应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、严禁关键技术扩散和设备行业专用等方面的约束条款。

系统交付

1. 应制订安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；
2. 应根据交付清单对所交接的设备、软件和文档等进行清点；
3. 应对负责运行维护的技术人员进行相应的技能培训；
4. 应提供建设过程中的文档和指导用户进行运行维护的文档。

供应链安全

1. 应制定供应链安全策略（包括采购策略等），并对安全策略的有效性进行持续监控；
2. 应在选择供应商前进行风险评估或现场检查；
3. 应在选择供应商前确保其具备相应的安全防护措施，包括但不限于其所提供的设备、平台系统等应为其所承载的业务提供相应的安全防护能力、其人员具有可信的背景审查结果；
4. 应与选定的服务供应商签订相关协议，明确供应链各方需履行的安全分工与责任；并规定具体服务内容和技术指标；
5. 应在服务协议中规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
6. 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已清除；
7. 应对外包开发的系统、软件等，在其上线应用前进行安全检测，留存检测报告；
8. 应要求供应商接受相关监督，确保供应商对其安全措施合规性进行持续监控并提供安全保障措施证明材料；
9. 应确保供应链安全事件信息或威胁信息能够及时传达到客户。
   * + - 1. 安全运维管理要求

环境管理

1. 应对机房的安全管理作出规定，指定特定的部门或人员负责机房物理环境安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
2. 应严禁在重要区域接待来访人员。

资产管理

1. 应建立并严格执行存储介质安全相关管理制度；
2. 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
3. 应建立存储介质相关资产台账（清单），对存储介质进行分类、分级标识；
4. 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
5. 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
6. 应对存储介质进行集中统一管理，详细记录介质领用、交回、维修、报废、销毁等环节；
7. 应对各种设备（包括备份和冗余设备）、线路等定期进行维护管理；
8. 应记录工业互联网设备的状态（包括外观、电量、指示灯等信息），对工业互联网设备进行现场维护（除尘、充电、修理等）；
9. 应对工业互联网设备部署环境的评估方法明确规定；
10. 应对工业互联网设备入库、存储、部署、携带、维修、丢失和报废等过程明确规定，并进行全程管理；
11. 应采用国家密码管理主管部门批准使用的密码算法和认证核准的密码产品；
12. 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
13. 应优先选择资质完备、经验丰富、安全可靠的运维服务商，应在供货合同中或以其他方式明确供应商应承担的网络安全责任和义务；
14. 应密切关注产品漏洞和补丁发布，及时进行软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入，在工业控制系统软件升级、补丁安装前要请专业技术机构进行安全检查评估和验证。

安全审计

1. 应对重要设备、平台、系统等启用安全审计功能，对重要的用户行为和重要安全事件进行审计。审计记录应包括事件的时间日期、用户、事件类型、事件简介及其他与审计相关的信息；
2. 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；审计记录中应避免明文记录敏感数据，如用户口令等；
3. 应确保审计记录的留存时间符合法律法规要求。

配置管理

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

安全事件处置

1. 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等；
2. 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件；
3. 应明确安全事件的报告和处置流程，制定安全事件报告和处置管理制度；
4. 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

应急工作要求

1. 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并根据实际情况适时进行评估和修订，每年进行一次评估和修订；
2. 应定期开展网络安全事件应急预案宣贯培训，确保相关人员熟悉应急预案，并进行应急预案的演练。
   * + 1. 物理和环境安全要求
          1. 物理位置选择
3. 机房和常规工业设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；
4. 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；
5. 机房外墙壁不应有对外的窗户。否则，应采用双层固定窗，并作密封、防水处理；
6. 室外工业互联网重要设备及控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中并紧固。
   * + - 1. 物理访问控制
7. 应在机房和工业设备放置场地出入口安排专人值守或部署电子门禁系统，控制、鉴别和记录进入的人员；
8. 应在重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网平台采取视频监控等手段。
9. 人员进出记录应至少保存3个月；机房出入口应有视频监控，监控记录应至少保存3个月。
   * + - 1. 防盗窃和防破坏
10. 应将设备或主要部件进行固定，并设置明显的不易除去的标记，如粘贴标签或铭牌、电子标签；
11. 应将通信线缆铺设在隐蔽安全处，可铺设在管道或线槽、线架中；
12. 主机房或重要设备区域应安装必要的防盗报警设施或设置有专人值守的视频监控系统，监控录像记录应至少保存3个月。
    * + - 1. 防雷击
13. 应将各类机柜、设施和设备等通过接地系统安全接地；
14. 应对室外控制设备电源、信号线路加装浪涌保护器等避雷装置。
    * + - 1. 防火

机房及工业设备放置场地应设置灭火设备和火灾自动报警系统。

* + - * 1. 防水和防潮

1. 应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透；
2. 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
   * + - 1. 防静电

应满足YD/T 1754-2008中3.2.7的相关要求。

* + - * 1. 温湿度控制

应满足YD/T 1754-2008中3.2.8的相关要求。

* + - * 1. 电力供应

应满足YD/T 1754-2008中3.2.10的相关要求。

* + - * 1. 电磁防护

1. 应满足YD/T 1754-2008中3.2.11的相关要求；
2. 电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰；
3. 室外工业互联网重要设备及控制设备放置应远离强电磁干扰、强热源等环境，如无法避免，应及时做好应急处置和检修，保证设备正常运行。
   * 1. 增强级防护要求
        1. 设备安全防护要求

除满足基本防护要求之外，还应符合以下要求：

* + - * 1. 工业主机安全防护要求

1. 应在不影响业务系统运行的前提下，定期对主机设备系统进行补丁更新，补丁安装前要进行完整性和可用性验证；
2. 应采用恶意代码防范手段，对于无法及时更新恶意代码库的场景，建议安装工业主机白名单防护软件；
3. 应对工业主机系统内的关键系统文件、业务文件、注册表信息等进行安全防护，对文件和注册表的操作权限进行管控；
4. 应对跨网使用的工业主机采取严格的管理措施；
5. 应通过主机外设安全管理技术手段对确需使用工业主机外设接口的设备实施访问控制，并对设备进行安全验证，以避免未授权的外设终端接入；
6. 应对临时接入的主机类设备采用技术管理手段进行访问控制，在进行安全扫描保证安全的前提下接入，并对设备的行为进行审计和管控。
7. 对临时接入的设备进行安全扫描，并留存安全扫描记录。
   * + - 1. 网络设备安全防护要求
8. 应实现网络设备的最小服务配置，并对配置文件进行定期离线备份；
9. 应及时更新网络设备系统和补丁，系统和补丁升级前进行安全性验证，并提前对重要文件进行备份；
10. 应在不影响业务的前提下，定期对网络设备系统进行漏洞扫描，对发现的安全漏洞及时处理；
11. 应对网络监控日志进行管理和审计分析，发现安全风险或问题，及时进行处理；
12. 应对网络设备采取登录失败处理措施，包括限制登录失败次数、连接超时自动退出、结束会话等；
13. 应对网络设备的远程管理采取必要的安全措施，对远程操作进行实时审计和管控，防止鉴别信息在传输过程中被窃取。
    * + - 1. 工业控制设备安全防护要求
14. 工业控制设备应具备对访问行为主体（人员、进程和设备）进行标识与鉴别的功能；
15. 工业控制设备自身应支持基于角色的访问控制策略配置，并对重要的安全性事件和重要生产活动进行审计；
16. 工业控制设备应具备数据完整性校验功能，防止对静态数据进行非授权写操作的保护机制（硬件或软件），并具备抵御数据包插入、丢失、重放、篡改的机制；
17. 对于控制设备内部的关键程序和文件，应具备对其进行加密和操作授权的功能，防止关键业务逻辑被窃取和篡改；
18. 对于需要远程维护的，要实行实时监管和审计，防止高危操作影响正常业务运行，加强在维护过程中文件传输和程序运行的管控，防止非正常文件输入和关键业务信息的输出。
19. 应部署统一配置管理平台对RTU、IED、DPU等现场测控设备进行集中管理；
20. 如现场测控设备直接或依靠其他工具提供备份功能，应进行应用级和系统级信息（包括系统安全状态信息）的备份。
21. 应对未使用的网络接口或串行通信接口进行关闭或封锁。
    * + 1. 控制安全防护要求

除满足基本防护要求之外，还应符合以下要求：

* + - * 1. 应用工业互联网的工业企业控制系统安全防护要求

1. 应定期自行对工业控制系统安全配置进行核查审计，避免因调试或其他操作导致配置变更后，未及时更新配置清单；
2. 应针对工业控制系统的开发、测试和生产分别提供独立环境，避免开发、测试环境中的安全风险引入生产系统；
3. 应部署具备对工业控制系统与网络进行状态监测、日志采集与事件管理、流量采集与行为分析、异常告警及关联分析等功能的网络安全监测设备，及时发现、报告并处理包括设备状态异常、恶意软件传播、异常流量、异常诊断日志、端口扫描、暴力破解等网络攻击或异常行为；
4. 应每半年针对工业控制系统进行一次全面的安全检查和评估，防止出现重大安全缺陷或安全漏洞；
5. 对发现的重大安全缺陷或安全漏洞，经过充分测试评估后，应及时进行修补或建立针对性的第三方检测防护技术措施；
   * + - 1. 组态软件安全要求
6. 应对组态软件的通信进行机密性保护；
7. 应采取措施保证组态软件的软硬件运行环境安全；
8. 应对组态软件加载的第三方库文件进行签名验证；
9. 应对组态软件进行第三方安全代码审计，对发现的安全缺陷或安全漏洞及时进行修补。
   * + - 1. 配置安全要求
10. 应具备恶意代码防护、服务器口令、服务器安全审计、服务器补丁更新、网络设备等口令接入控制及统一防护等方面的策略；
11. 应建立独立的配置变更管理服务器，用于存放配置信息及备份的配置，按照约定的周期备份配置，并定期开展备份恢复测试；
12. 应严格管理配置管理库的访问权限，核心配置信息要控制知悉范围，配置管理库的完整性、可用性要得到保证；
13. 应建立机制定期评审正在运行的配置，以发现潜在的风险或任何可能优化配置的改进点。
    * + - 1. 智能装备控制安全要求
14. 现场重要设备应具有完善的控制指令来源识别验证、访问控制功能；
15. 现场重要设备应支持异常指令、状态等的审计数据上报；
16. 工业互联网平台与其直接控制的现场重要设备（如AGV、工业机器人、CNC数控机床、工业网关等）通信时，应对带宽进行限制。
    * + 1. 网络安全防护要求
           1. 架构安全要求

除满足基本防护要求之外，还应符合以下要求：

1. 应将控制系统网络与非控制系统网络进行物理分区，将关键控制系统网络与非关键控制系统网络进行物理分区；
2. 应支持在不与非控制系统网络相连的情况下，为关键控制系统网络提供网络服务；
3. 应能够按照业务服务的重要程度分配带宽，优先保障重要业务；
4. 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证信息系统的可用性。
   * + - 1. 边界安全要求

除满足基本防护要求之外，还应符合以下要求：

1. 应在控制网络和非控制网络的边界防护机制失效时，能阻止所有边界通信；
2. 应在控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警，并保障不影响关键设备通讯；
3. 当使用无线设备连接控制网络和非控制网络，或连接控制网络内不同安全域时，应对无线设备采取边界防护措施，包括但不限于身份标识和鉴别、访问控制等；
4. 应在网络边界节点处对恶意代码进行检测和清除，并维护恶意代码防护主程序及特征库的升级和更新。
   * + - 1. 通信安全要求

除满足基本防护要求之外，还应符合以下要求：

1. 在工业企业内部网络进行通信数据传输时，应在通信前对通信的双方进行验证或认证。
   * + 1. 数据安全防护要求

同6.1.4的要求。

* + - 1. 软件安全防护要求
         1. 工业互联网设备固件安全要求

a）应建立各类工业互联网设备的主控芯片型号、软件版本、操作系统（如有）名称及版本等设备底层信息台账；

b）依据安全台账信息，应定期检查工业互联网安全漏洞平台披露的漏洞信息，如漏洞描述关联设备相关信息，应及时采取缓解措施。

c）设备固件升级前应利用固件安全检测工具动态扫描漏洞后门，提前发现越权执行、缓冲区溢出、远程命令执行、密钥泄露、隐藏后门、配置不当等各种安全隐患。

* + - * 1. 生产控制软件安全要求

a） 应当在保证生产控制软件可靠、稳定运行的基础上，提高生产控制软件自身的安全防护能力；

b） 应当具备容错机制，在发生单点故障时，应当能继续提供生产控制功能。

* + - * 1. 本地部署平台软件安全要求

a） 应当在平台内部区分不同模块的重要程度，针对平台内部核心功能模块，应采用审核或白名单机制，只允许审核通过的设备访问核心功能模块；针对平台内部对外提供服务的功能模块，应当具备注册机制，掌握设备接入情况，可以在发生异常情况时，及时拒绝异常设备接入；

b） 应当采取措施保障虚拟机安全，包括虚拟机隔离，实时监控虚拟机资源使用情况等；

c） 应当具备安全态势感知和呈现能力，可以对平台内部及工业APP实现安全管控。

* + - * 1. 第三方平台软件安全要求

a） 应当具备入侵检测能力，能够及时阻断来自第三方平台的安全入侵，防止攻击者进入系统；

b） 应当具备重要数据的监测能力，当重要数据进入第三方平台时，系统能记录数据的流向并给出风险提示。

* + - * 1. 工业APP安全要求

a） 应当在部署工业APP之前，检测工业APP的潜在安全漏洞，尽量减小安全隐患；

b） 应当具备容错机制，在发生单点故障时可继续提供基本功能。

* + - 1. 网络安全管理要求
         1. 安全策略和管理制度

除满足基本防护要求之外，还应符合以下要求：

应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

* + - * 1. 安全管理机构和人员要求

除满足6.1.6.2的要求之外，还应符合以下要求：

安全管理机构

同6.1.6.2.1的要求。

人员要求

1. 应成立指导和管理安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
2. 应配备专职安全管理员，不可兼任，关键事务岗位应配备多人共同管理；
3. 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
4. 应定期全面开展安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
5. 应确定安全检查内容实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
6. 应从内部工作一年以上的人员中选拔从事关键岗位的人员；
7. 应对被录用人员具备的技术技能进行考核，应与被录用人员签订保密协议，与关键岗位人员签订岗位责任协议；
8. 人员离岗前，应办理正式的调离手续，并签署调离后的保密承诺；
9. 应针对不同岗位开展针对性网络安全相关培训，应定期对相关人员进行技能考核；
10. 接触系统的外部人员应签署保密协议，严禁非授权操作和获取敏感信息，严禁访问关键区域或系统。
    * + - 1. 安全建设管理要求

除满足基本防护要求之外，还应符合以下要求：

定级

同6.1.6.3.1的要求。

安全方案设计

1. 应根据安全防护对象的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
2. 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

产品采购和使用

1. 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
2. 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

软件开发

1. 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
2. 应制定代码编写安全规范，要求开发人员参照规范编写代码；
3. 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
4. 应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
5. 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
6. 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

系统交付

安全测试报告应包含密码应用安全性测试相关内容。

供应链安全

1. 应定期评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
2. 应与选定的服务供应商签署保密协议，要求其不得泄露客户数据和业务系统的相关重要信息；
3. 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制；
4. 应将网络安全防护设施建设、运行维护，日常网络安全管理，网络安全检查，网络安全应急演练等费用纳入部门年度预算，保证网络安全经费投入。
   * + - 1. 安全运维管理要求

除满足6.1.6.4的要求之外，还应符合以下要求：

环境管理

1. 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；
2. 应加强对工业互联网设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

资产管理

1. 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
2. 应对信息分类与标识方法明确规定，并对信息的使用、传输和存储等进行规范化管理；
3. 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
4. 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
5. 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程。

安全审计

1. 应能对远程访问企业内部网络的用户行为进行行为审计和数据分析；
2. 应对审计进程进行保护，防止未经授权的中断；
3. 审计记录的留存时间应不少于6个月。

配置管理

应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

安全事件处置

对造成业务中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

应急工作要求

1. 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
2. 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，对应急预案进行评估和适用性修订；
3. 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。
   * + 1. 物理和环境安全要求
          1. 物理位置选择

除满足6.1.7.1的要求之外，还应满足：

1. 机房场地不应设在建筑物用水设备的隔壁或下层，否则应加强防水和防潮措施；
2. 确保工业互联网平台服务器及运行关键业务和数据的物理设备位于中国境内；
3. 对于存在爆炸危险的生产车间（装置），主机房、现场控制室、现场机柜室应位于爆炸危险区域外。
   * + - 1. 物理访问控制
4. 应在机房和工业设备放置场地出入口安排专人值守或部署电子门禁系统，控制、鉴别和记录进入的人员；
5. 应在重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网平台采取视频监控等手段。
6. 针对重要核心工业互联网软硬件所在区域或工业互联网平台（如工程师站、数据库、服务器、工业控制设备等）应划分重点物理安全防护区域；
7. 机房出入口应当安排专人负责管理，人员进出记录应至少保存3个月；机房出入口应有视频监控，监控记录应至少保存3个月。
   * + - 1. 防盗窃和防破坏

除满足6.1.7.3的要求之外，还应满足：

1. 应对机房设置监控报警系统或设置有专人值守的视频监控系统，非7\*24小时人员值守和巡查的 机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵及时显示入侵部位，并驱动声光报警装置；
2. 应将室外控制设备安装在具有防盗能力的箱体或装置中；
3. 拆除或封闭工业主机上不必要的USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。
   * + - 1. 防雷击

同6.1.7.4的要求。

* + - * 1. 防火

1. 机房及工业设备放置场地应设置灭火设备和火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火；
2. 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
   * + - 1. 防水和防潮

除满足6.1.7.6的要求之外，还应满足：

应安装对水敏感的检测仪表或元件，对机房及工业设备放置场地进行防水检测和报警。

* + - * 1. 防静电

应满足YD/T 1754-2008中3.3.7的相关要求。

* + - * 1. 温湿度控制

同6.1.7.8的要求。

* + - * 1. 电力供应

除满足6.1.7.9的要求之外，还应满足：

1. 应配备UPS，在配有发电机等后备电源的情况下，UPS供电能力能支持到后备电源开始供电；备用电力供应的实际供电能力应满足主要设备和环境控制设备在断电情况下正常运行至少2个小时；
2. 应设置冗余或并行的电力电缆线路为计算机系统供电；应至少采用双路市电，且不能来自同一变电站。
   * + - 1. 电磁防护

同6.1.7.10的要求。