工 业 互 联 网 产 业 联 盟 标 准

AII/003-2018

工业互联网 安全总体要求

General Security Requirements for Industrial Internet

工业互联网产业联盟

（2018 年 2 月 2 日发布）

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目　录

前　　言

本标准是工业互联网安全防护系列标准之一。

—工业互联网　　安全总体要求

—工业互联网　　安全接入要求

—工业互联网平台　安全防护要求

—工业互联网　　安全能力成熟度评估规范

—工业互联网　　数据安全保护要求

随着技术的发展，还将制定后续的相关标准。

标准牵头单位：中国信息通信研究院

标准起草单位和主要起草人：

中国信息通信研究院：李艺、田慧蓉、罗成

华为技术有限公司：王雨晨、耿涛

北京奇虎科技有限公司：陶耀东、郭颖

中国移动通信集团有限公司：张峰

中兴通讯股份有限公司：黄树强

中国电子信息产业集团有限公司第六研究所：卢凯

航天云网科技发展有限责任公司：于文涛、邹萍、姜海森、梁栋

富士康科技集团：陈金星

用友网络科技股份有限公司：杨宝刚

三一集团：彭卓、张声勇

北京和利时智能技术有限公司：龚涛

中国科学院沈阳自动化研究所：李栋

海尔集团：陈云峰、张海港

工业互联网 安全总体要求

1 范围

本标准规定了工业互联网应用场景下各组成对象不同安全等级的安全防护要求。

本标准适用于工业现场设备、工业控制系统、工业互联网平台及工业应用程序。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 22239-XXXX	信息安全技术 网络安全等级保护基本要求
YD/T 1729-2008	电信网和互联网安全等级保护实施指南
工业互联网产业联盟报告	工业互联网平台白皮书（2017）

3 缩略语

下列缩略语适用于本文件。

II	工业互联网	Industrial Internet

4 术语和定义

下列术语和定义适用于本文件。

4.1

工业互联网　Industrial Internet

工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

4.2

工业互联网平台　Industrial Internet Platform

工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台。

4.3

工业应用程序 Industry Application Program

指可实现包括工业设计、生产、管理、服务等在内能力的工业业务系统或移动应用程序。

4.4

网络安全　Network Security

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

5 工业互联网网络安全防护场景概述

5.1 工业互联网网络安全防护范围

工业互联网从防护对象可分为现场设备、工业控制系统、网络基础设施、工业互联网应用、工业数据五个层级，各层所包含对象纳入工业互联网安全防护范围。

- 设备安全：指工业智能装备和智能产品的安全，包括操作系统与相关应用软件安全以及硬件安全等。

- 控制安全：指生产控制安全，包括控制协议安全与控制软件安全等。
- 网络安全：指工厂内有线网络、无线网络的安全，以及工厂外与用户、协作企业等实现互联的公共网络安全。
- 应用安全：指支撑工业互联网业务运行的平台安全及应用程序安全等。
- 数据安全：指工厂内部重要的生产管理数据、生产操作数据以及工厂外部数据（如用户数据）等各类数据的安全。

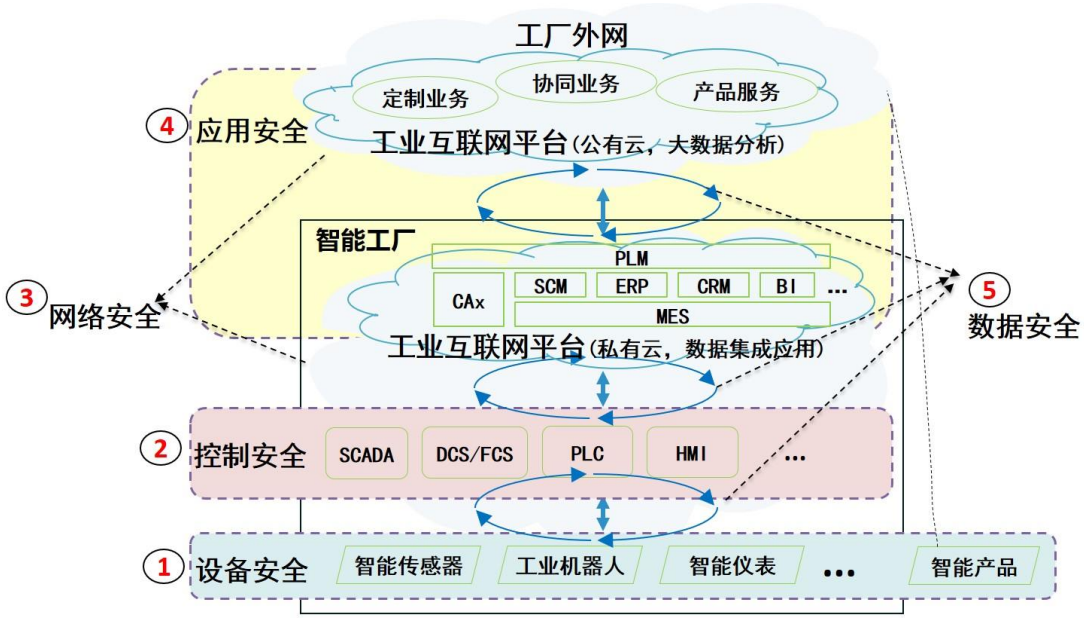

图1 工业互联网安全防护场景

5.2 工业互联网安全防护内容

工业互联网安全防护旨在加强工业互联网各层防护对象安全水平，保障系统网络安全运营，防范网络攻击。工业互联网安全防护内容具体包括：

- 设备安全：包括设备及运维用户的身份鉴别、访问控制，以及设备的入侵防范、安全审计等。
- 控制安全：包括控制协议的完整性保护、控制软件的身份鉴别、访问控制、入侵防范、安全审计等。
- 网络安全：包括网络与边界的划分隔离、访问控制、机密性与完整性保护、异常监测、入侵防范、安全审计等。
- 应用安全：包括工业互联网平台及工业应用程序的访问控制、攻击防范、入侵防范、行为管控、来源控制等。
- 数据安全：包括数据机密性保护、完整性保护、数据备份恢复、数据安

全销毁等。

6 工业互联网定级对象和安全等级确定

我国具有管辖权的工业互联网系统为安全等级定级对象。

运营单位应根据 YD/T 1729-2008 《电信网和互联网安全等级保护实施指南》附录A中确定安全等级的方法对工业互联网系统定级。可根据相应的社会影响力、所提供服务的重要性、服务用户数的大小进行定级。

对于工业互联网系统的安全保护分为以下五个等级：

第一级，工业互联网系统受到破坏后，会对系统提供商、个人及企业用户等的合法权益造成轻微损害，但不损害国家安全、社会秩序和公共利益。

第二级，工业互联网系统受到破坏后，会对系统提供商、个人及企业用户等的合法权益产生严重损害，或者对社会秩序、经济运行和公共利益造成轻微损害，但不损害国家安全。

第三级，工业互联网系统受到破坏后，会对系统提供商、个人及企业用户等的合法权益产生特别严重损害，或者对社会秩序、经济运行和公共利益造成严重损害，或者对国家安全造成损害。

第四级，工业互联网系统受到破坏后，会对社会秩序、经济运行和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，工业互联网系统受到破坏后，会对国家安全造成特别严重损害。

7 工业互联网安全防护要求

7.1 第 1 级

7.1.1 设备安全防护要求

a) 设备准入控制

应采用鉴别机制对接入工业互联网中的设备身份进行鉴别，确保数据来源于真实的设备。

b) 设备访问控制

应通过制定安全策略如访问控制列表，实现对接入工业互联网中设备的访问控制。

c) 运维用户身份鉴别

1) 应对登录设备进行运维的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

2) 对于登录设备进行运维的过程应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

d) 运维用户访问控制

1) 应对登录设备进行运维的用户分配账户和权限；

2) 应重命名或删除默认账户，修改默认账户的默认口令；

3) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

e) 入侵防范

1) 应遵循最小安装的原则，仅为设备安装需要的组件和应用程序；

2) 应关闭设备中不需要的系统服务、默认共享和高危端口。

7.1.2 控制安全防护要求

a) 控制协议完整性保护

对于控制协议应采取完整性保证机制，确保控制协议中的各类指令不被非法篡改和破坏。

b) 控制软件用户身份鉴别

1) 应对登录控制软件进行操作的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

2) 对于登录控制软件进行操作的过程应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

c) 控制软件用户访问控制

1) 应对登录控制软件进行运维的用户分配账户和权限；

2) 应重命名或删除默认账户，修改默认账户的默认口令；

3) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

d) 入侵防范

1) 控制软件应遵循最小安装的原则，仅安装需要的组件和程序；

2) 应关闭控制软件所在主机中不需要的系统服务、默认共享和高危端口。

7.1.3 网络安全防护要求

7.1.3.1 工厂内部网络安全防护要求

a) 区域划分与隔离

工厂内部网络应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

b) 数据传输完整性

应采用适应工厂内部网络特点的完整性校验机制，实现对网络数据传输完整性保护。

7.1.3.2 工厂外部网络安全防护要求

a) 数据传输完整性

应采用常规校验机制检验网络数据传输的完整性，并能发现其完整性被破坏的情况。

b) 数据传输保密性

应采用密码技术支持的数据保密机制，实现对网络中传输数据的保密性保护。

7.1.3.3 边界防护要求

a) 网络边界隔离

工厂内部网络与工厂外部网络之间应划分为两个区域，区域间应采用技术隔离手段。

b) 网络边界访问控制

1) 应在网络边界根据访问控制策略设置访问控制规则，保证跨越网络边界的访问和数据流通过边界防护设备提供的受控接口进行通信，默认情况下受控接口拒绝所有通信；

2) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

3) 应根据网络边界访问控制规则，通过检查数据包的源地址、目的地址、源端口、目的端口、和协议等，确定是否允许该数据包通过该区域边界；

4) 工厂内部网络与工厂外部网络之间应采用访问控制机制，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

7.1.4 应用安全防护要求

a) 用户身份鉴别

1) 应对使用工业互联网平台与工业应用程序的用户身份进行标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

2) 工业互联网平台及工业应用程序的登录过程应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

b) 访问控制

1) 应提供访问控制功能，对使用工业互联网平台及工业应用程序的用户分配账户及相应的访问操作权限；

2) 应重命名或删除默认账户，修改默认账户的默认登录口令；

3) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

c) 合规性检验

对于工业互联网平台及工业应用程序应提供数据合规性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合其设定要求。

d) 应用管控

工业应用程序用户应具有选择应用程序安装、运行的功能。

e) 应用来源保证

工业互联网平台运营商应保证终端设备安装、运行的工业应用程序来自可靠证书签名或可靠分发渠道。

7.1.5 数据安全防护要求

a) 数据保密性保护

应采用密码技术支持的保密性保护机制对存储数据的保密性提供保护。

b) 数据完整性保护

1) 应采用常规校验机制检验存储数据的完整性，以发现其完整性是否被破坏；

2) 应确保工业互联网平台数据迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

c) 数据备份与恢复

1) 应提供对重要数据的本地数据备份与恢复功能，保证数据副本之间的一致性，且备份数据应采取与原数据一致的安全保护措施；

2) 应提供查询工业互联网平台客户数据及备份存储位置的方式。

d) 数据销毁

工业互联网平台及工业应用程序应提供数据销毁机制，并明确销毁方式和销毁要求。

7.2 第 2 级

7.2.1 设备安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 设备准入控制

若存在需要对接入工业互联网中的设备进行远程管理的，应采取必要措施，防止身份鉴别信息在网络传输过程中被窃听。

b) 运维用户访问控制

应对管理设备的用户授予其所需的最小权限，并实现对管理设备的用户的权限分离。

c) 设备安全审计

1) 应启用安全审计功能，审计覆盖到对设备进行运维的每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

d) 入侵防范

1) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

2) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

7.2.2 控制安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 控制软件安全审计

1) 应启用安全审计功能，审计覆盖到对控制软件进行操作的每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

b) 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

c) 资源控制

应限制单个用户或进程对系统资源的最大使用限度。

7.2.3 网络安全防护要求

7.2.3.1 工厂内部网络安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 数据传输完整性保护

应采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。

b) 网络异常监测

应对网络通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警。

c) 无线网络攻击的防护

应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，并对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽。

d) 网络入侵防范

应在关键网络节点处部署入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警。

e) 恶意代码防范

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

f) 网络安全审计

1) 应在关键网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

7.2.3.2 工厂外部网络安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 网络入侵防范

应在关键网络节点处部署入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警。

b) 恶意代码防范

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

c) 网络安全审计

1) 应在关键网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

7.2.3.3 边界防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 网络边界访问控制

应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。

b) 网络边界安全审计

1) 应在网络边界进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

c) 网络边界恶意代码防范

应在网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

7.2.4 应用安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 用户身份鉴别

1) 应使用密码技术对鉴别数据进行保密性和完整性保护。

2) 应强制用户首次登录时修改初始口令；

3) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。

b) 访问控制

1) 工业互联网平台应为工业应用程序提供访问控制授权能力；

2) 应根据访问控制策略，对工业互联网平台开发者、工业应用程序及其用户调用工业互联网平台开发接口实施访问控制。

c) 安全审计

1) 应提供安全审计功能，审计覆盖到使用工业互联网平台及工业应用程序的每个用户，对重要的用户行为和重要安全事件进行审计；

2) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3) 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；

4) 应确保审计记录的留存时间符合法律法规要求。

d) 运维环境管理

1) 工业互联网平台的运维地点应位于中国境内，境外对境内工业互联网平台实施运维操作应遵循国家相关规定；

2) 工业互联网平台运维过程产生的配置数据、日志信息等存储于中国境内，如需出境应遵循国家相关规定。

e) 应用管控

1) 应设置针对工业应用程序的白名单功能，根据应用程序白名单控制应用程序的安装、运行；

2) 应具有应用程序权限控制功能，应能控制应用程序对终端设备中资源的访问；

3) 应只允许可靠证书签名的应用程序安装和运行。

f) 应用来源保证

1) 工业互联网平台运营商应保证终端设备安装、运行的工业应用程序由可靠的开发者开发；

2) 工业互联网平台运营商应验证开发工业应用程序的签名证书的合法性。

g) 应用健壮性保证

在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。

h) 应用资源控制

1) 工业互联网平台及工业应用程序应具备会话超时自动结束功能，当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

2) 应能够对工业互联网平台及工业应用程序的最大并发会话连接数进行限制；

3) 应能够对单个账户的多重并发会话进行限制。

4) 应能够对用户或进程对终端设备系统资源的最大使用限度进行限制，防止终端设备被提权。

i) 应用上线前检测

应在工业互联网平台及工业应用程序上线前对其安全性进行测试，对可能存在的恶意代码进行检测。

7.2.5 数据安全防护要求

除满足第 1 级的要求之外，还应符合以下要求：

a) 数据使用

工业互联网平台应提供数据脱敏和去标识化的工具或服务组件技术。

b) 数据备份恢复

工业互联网平台应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

c) 数据销毁

1) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

2) 应保证工业互联网平台用户所使用的内存和存储空间在回收时得到完全清除；

3) 工业互联网平台用户删除业务数据时，平台运营商应确保平台中存储的所有副本被删除；

4) 工业互联网平台进行数据整体迁移的过程中，应杜绝数据残留。

d) 个人信息保护

1) 工业互联网平台运营商应仅采集和保存业务必需的用户个人信息；

2) 工业互联网平台运营商应禁止未授权访问和非法使用用户个人信息。

3) 应确保工业互联网平台用户的账户信息、鉴别信息、系统信息存储于中国境内，如需出境应遵循国家相关规定。

7.3 第 3 级

7.3.1 设备安全防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 设备安全审计

在有冗余的重要应用环境，可对部署的多重设备进行实时审计跟踪，确保及时捕获信息安全事件信息并报警。

7.3.2 控制安全防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 控制协议完整性保护

控制协议应能识别和防范破坏控制协议完整性的攻击行为。

b) 控制软件安全审计

应对审计进程进行保护，防止未经授权的中断。

c) 入侵防范

应能够检测到对重要控制系统进行入侵的行为，并在发生严重入侵事件时提供报警。

d) 恶意代码防范

应采用免受恶意代码攻击的技术措施或可信验证机制对控制系统程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

7.3.3 网络安全防护要求

7.3.3.1 工厂内部网络安全防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 数据传输保密性保护

应采用适应工厂内部网络特点的密码技术支持的保密性保护机制，以实现工

厂内部网络数据传输保密性保护。

b) 网络访问控制

应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。

c) 网络入侵防范

1) 应在关键网络节点处检测、防止或限制从节点内外侧发起的网络攻击行为；

2) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

3) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

d) 网络安全审计

应能对远程访问工厂内部网络的用户行为进行行为审计和数据分析。

7.3.3.2 工厂外部网络安全防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 网络访问控制

应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。

b) 网络入侵防范

1) 应在关键网络节点处检测、防止或限制从节点内外侧发起的网络攻击行为；

2) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

3) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

c) 网络集中管控

1) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

2) 应对分散在各个网络设备上的审计数据进行收集汇总和集中分析；

3) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

4) 应能对网络中发生的各类安全事件进行识别、报警和分析。

7.3.3.3 边界防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 网络边界访问控制

1) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则；

2) 对于工厂内部网络与工厂外部网络之间只存在单向数据传输的，网络间应采用单向的技术隔离手段。

7.3.4 应用安全防护要求

除满足第 2 级的要求之外，还应符合以下要求：

a) 用户身份鉴别

应采用口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别。

b) 安全审计

应对审计进程进行保护，防止未经授权的中断。

c) 应用来源保证

对于工业互联网平台及工业应用程序上线前的安全测试报告应包含密码应用安全性测试相关内容。

7.3.5 数据安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 数据保密性保护

1) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

2) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

3) 应使用密码技术确保工业互联网平台迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露。

b) 数据完整性保护

1) 应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

2) 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

3) 应使用校验码或密码技术确保工业互联网平台迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

c) 数据使用

1) 应采用技术手段，确保数据源的真实可信；

2) 应对导入或者其他数据采集方式收集到的数据进行检测，避免出现恶意数据输入；

3) 应确保在数据清洗和转换过程中对重要数据进行保护,以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复，受保护的数据范围包括但不限于鉴别数据、重要业务数据和重要个人信息等；

4) 应采用技术手段防止在数据应用过程识别出鉴别信息；

5) 应采用技术手段限制在终端设备输出重要数据，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

6) 应采用技术手段防止进行未授权的数据分析；

d) 数据备份恢复

1) 工业互联网平台应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

2) 工业互联网平台应提供重要数据处理系统的热冗余，保证系统的高可用性；

3) 应保证不同工业互联网平台用户的审计数据隔离存放；

4) 应为工业互联网平台用户将业务系统及数据迁移到其他平台和本地系统提供技术手段，并协助完成迁移过程；

5) 工业互联网平台运营商的数据存储服务应确保平台用户数据存在若干个可用的副本，各副本之间的内容应保持一致。

e) 数据销毁

1) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

2) 工业互联网平台应提供基于数据分类分级的数据销毁机制，并明确销毁方式和销毁要求。

f) 数据溯源

1) 应跟踪和记录数据采集、处理、分析和挖掘等过程，确保溯源数据能重现相应过程；

2) 溯源数据应能支撑数据业务要求和合规审计要求；

3) 应采用技术手段保证溯源数据真实性和保密性。

7.4 第 4 级

7.4.1 设备安全防护要求

同第 3 级要求。

7.4.2 控制安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 控制逻辑完整性保护

应采用由密码技术支持的完整性校验机制，以实现对控制逻辑完整性保护，并在发现完整性被破坏时进行恢复。

7.4.3 网络安全防护要求

7.4.3.1 工厂内部网络安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 非法外连检测

应能够对工厂内部网络中的用户或网络设备非授权连接到工厂外部网络或因特网的行为进行限制或检查，并对其进行有效阻断。

7.4.3.2 工厂外部网络安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 数据传输密码管理

应基于密码模块对重要通信过程进行密码运算和密钥管理。

7.4.3.3 边界防护要求

同第 3 级要求。

7.4.4 应用安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 用户身份鉴别

工业互联网平台及工业应用程序登录用户执行重要操作时应再次进行身份鉴别。

7.4.5 数据安全防护要求

除满足第 3 级的要求之外，还应符合以下要求：

a) 数据抗抵赖

在工业互联网平台及可能涉及法律责任认定的工业应用程序中，应采用密码

技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

b) 数据备份恢复

工业互联网平台应建立异地灾难备份中心，提供业务应用的实时切换。

7.5 第 5 级

由于 GB/T 22239-XXXX《信息安全技术 网络安全等级保护基本要求》中未对第五级保护对象的安全要求进行描述，因此本标准中不对第五级等级保护对象的安全要求进行描述。

参考文献

[1] YD/T 1728-2008 电信网和互联网安全防护管理指南
[2] YD/T 1730-2008 电信网和互联网安全风险评估实施指南
[3] YD/T 1731-2008 电信网和互联网灾难备份及恢复实施指南
[4] YD/T 1754-2008 电信网和互联网物理环境安全防护要求
[5] YD/T 1756-2008 电信网和互联网管理安全防护要求
[6] YD/T 2052-2009 域名系统安全防护要求
[7] YD/T 1736-2009 互联网安全防护要求