ICS 35.020
A 90

中华人民共和国国家标准

GB/T 35317—2017

公安物联网系统信息安全等级保护要求

Information classified security protection requirements for systems of IoTPS

2017-12-29 发布　　2017-12-29 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：公安部第三研究所、公安部第一研究所、无锡物联网产业研究院、工业和信息化部电子工业标准化研究院。

本标准主要起草人：陶源、齐力、杨明、唐前进、李末岩、于春兰、尚旭光、王李乐、张宇翔、郑国刚、郭俸明、任婷、尹湘培、陆洪波、李程远、杜大海、李秋香、陈书义、龚洁中。

公安物联网系统信息安全等级保护要求

1 范围

本标准规定了不同安全等级的公安物联网系统信息安全等级保护的技术和管理要求。

本标准适用于公安物联网系统的安全建设和监督管理。

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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069—2010 信息安全技术 术语

GA/T 1266—2015 公安物联网术语

3 术语和定义

GB 17859—1999、GB/T 22239—2008、GB/T 22240—2008、GB/T 25069—2010 和 GA/T 1266—2015 界定的术语和定义适用于本文件。

4 安全保护等级概述

4.1 安全保护等级

公安物联网系统安全保护等级的确定应符合 GB/T 22240—2008 的规定。

4.2 不同等级的安全保护能力

公安物联网系统不同等级的安全保护能力应符合 GB/T 22239—2008 中 4.2 的要求，本标准仅对 1 级～4 级的安全保护要求做出规定。

4.3 安全保护要求的三种类型

公安物联网系统的安全保护类型使用标记符合 GB/T 22239—2008 中 4.4 要求。

5 第一级要求

5.1 技术要求

5.1.1 物理安全

5.1.1.1 基本要求

物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、温湿度控制、电力供应应符合

GB/T 22239—2008 中 5.1.1 的要求。

5.1.1.2 物理位置的选择(G1)

公安物联网户外设备应选择部署在不易被破坏、被移除的位置。

5.1.1.3 防盗窃和防破坏(G1)

防盗窃和防破坏除基本要求外,公安物联网户外设备还应采取专用工具且不易拆卸的方式安装。

5.1.1.4 感知终端的物理安全(G1)

感知终端的物理安全应满足以下要求:

a) 所处的物理环境不对感知终端造成物理破坏;

b) 能准确反映所处的物理环境状态。

5.1.2 网络安全

5.1.2.1 基本要求

结构安全、访问控制和网络设备防护应符合 GB/T 22239—2008 中 5.1.2 的要求。

5.1.2.2 访问控制(S1)

访问控制除基本要求外,还应满足:

a) 设置感知终端入网访问控制;

b) 远程配置感知终端、物联网网关的软件应用时,进行访问控制。

5.1.2.3 感知设备防护(A1)

应采取措施防止感知设备被破坏。

5.1.2.4 设备标识(S1)

应对感知设备建立系统内唯一的标识。

5.1.2.5 组认证(S1)

宜对感知终端构成的组提供组标识的能力。

5.1.2.6 数据源认证(S1)

宜确保信息来源于正确的感知终端和物联网网关。

5.1.2.7 异构网接入(S1)

应对异构网络的接入进行安全检测。

5.1.3 主机安全

身份鉴别、访问控制、入侵防范和恶意代码防范应符合 GB/T 22239—2008 中 5.1.3 的要求。

5.1.4 应用安全

5.1.4.1 基本要求

身份鉴别、访问控制、通信完整性和软件容错应符合 GB/T 22239—2008 中 5.1.4 的要求。

5.1.4.2 身份鉴别(S1)

身份鉴别除基本要求外,还需满足:

a) 应建立感知终端的标识管理机制;

b) 宜对来自于感知终端的信息采取先验证信息源再处理的机制。

5.1.4.3 感知终端软件更新(A1)

感知终端软件更新应满足以下要求:

a) 具有适应公安物联网应用业务扩展和安全加固的更新机制;

b) 具有回退机制,保证未正常更新的感知终端能恢复到更新前的状态。

5.1.5 数据安全及备份恢复

5.1.5.1 基本要求

数据完整性、备份和恢复应符合 GB/T 22239—2008 中 5.1.5 的要求。

5.1.5.2 数据完整性(S1)

数据完整性除基本要求外,还应能够检测到感知终端生存信息在传输过程中完整性受到破坏。

5.1.5.3 数据可用性(A1)

应保证感知设备之间通信数据的可用性。

5.2 管理要求

5.2.1 安全管理制度

管理制度、制定和发布应符合 GB/T 22239—2008 中 5.2.1 的要求。

5.2.2 安全管理机构

岗位设置、人员配备、授权和审批、沟通和合作应符合 GB/T 22239—2008 中 5.2.2 的要求。

5.2.3 人员安全管理

人员录用、人员离岗、安全意识教育和培训、外部人员访问管理应符合 GB/T 22239—2008 中 5.2.3 的要求。

5.2.4 系统建设管理

5.2.4.1 基本要求

系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付和安全服务商选择应符合 GB/T 22239—2008 中 5.2.4 的要求。

5.2.4.2 产品采购和使用(G1)

产品采购和使用除基本要求外,感知设备还应符合国家的有关规定。

5.2.4.3 自行研发感知设备(G1)

自行研发感知设备应满足以下要求:

a） 主要部件参数满足系统功能需求；
b） 研发环境与实际运行环境物理分开；
c） 提供感知设备软、硬件设计的相关文档，并由专人负责保管。

5.2.4.4 外包研发感知设备（G1）

外包研发感知设备应满足以下要求：
a） 根据研发需求检测感知设备软、硬件质量；
b） 在软件安装之前检测软件包中可能存在的恶意代码；
c） 要求研发单位提供软、硬件设计的相关文档和使用指南；
d） 根据研发单位提供的硬件设计图审查实物与设计是否一致。

5.2.5 系统运维管理

5.2.5.1 基本要求

环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、备份与恢复管理和安全事件处置应符合 GB/T 22239—2008 中 5.2.5 的要求。

5.2.5.2 环境管理（G1）

环境管理除基本要求外，还应满足以下要求：
a） 定期巡视感知终端、物联网网关的部署环境，对可能影响感知终端、物联网网关正常工作的环境异常进行记录和维护；
b） 制定感知终端、物联网网关入库、存储、部署、携带、维修、丢失和报废等管理制度，并进行全程管理。

5.2.5.3 备份与恢复管理（G1）

备份与恢复管理除基本要求外，还应规定感知终端、物联网网关备份信息的备份方式、备份频度、存储介质、保存期等。

6 第二级要求

6.1 技术要求

6.1.1 物理安全

6.1.1.1 基本要求

物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、温湿度控制、电力供应、电磁防护应符合 GB/T 22239—2008 中 6.1.1 的要求。

6.1.1.2 物理位置的选择（G2）

物理位置的选择除基本要求外，公安物联网户外设备应选择部署在不易被破坏、被移除的位置。

6.1.1.3 防盗窃和防破坏（G2）

防盗窃和防破坏除基本要求外，公安物联网户外设备还应采取专用工具且不易拆卸的方式安装。

6.1.1.4 感知终端的物理安全(G2)

感知终端的物理安全应满足以下要求：

a) 所处的物理环境不对感知终端造成物理破坏；

b) 能准确反映所处的物理环境状态。

6.1.1.5 物联网网关的物理安全(G2)

物联网网关应满足以下要求：

a) 所在物理环境具备防火、防静电、防潮和防水的能力；

b) 固定主要部件，并设置明显的不易除去的标记。

6.1.1.6 防雷击(G2)

防雷击除基本要求外，公安物联网户外设备还应设置避雷或防雷措施。

6.1.2 网络安全

6.1.2.1 基本要求

结构安全、访问控制、安全审计、边界完整性检查和入侵防范应符合 GB/T 22239—2008 中 6.1.2 的要求。

6.1.2.2 访问控制(S2)

访问控制除基本要求外，还应满足：

a) 设置感知终端入网访问控制；

b) 远程配置感知终端、物联网网关的软件应用时，进行访问控制；

c) 对感知终端接入网络资源设置访问控制机制；

d) 防止感知终端和物联网网关的资源被非法访问和使用。

6.1.2.3 感知设备防护(A2)

应采取措施防止感知设备被破坏和篡改。

6.1.2.4 设备标识(S2)

设备标识应满足以下要求：

a) 对感知设备建立系统内唯一的标识信息；

b) 具有对连接的感知设备进行身份鉴别的能力。

6.1.2.5 感知设备认证(S2)

感知设备认证应满足以下要求：

a) 对感知设备建立注册机制；

b) 感知设备需在系统认证之后才可以接入网络中。

6.1.2.6 组认证(S2)

应对感知终端构成的组提供组标识和组认证的能力。

6.1.2.7 数据源认证(S2)

应确保信息来源于正确的感知终端和物联网网关。

6.1.2.8 异构网接入(S2)

异构网接入应满足以下要求：

a) 对异构网络的接入进行安全检测；

b) 具有拒绝恶意网络节点的接入能力。

6.1.2.9 终端位置隐私保护(G2)

应具有感知终端物理位置和网络地址隐私保护的能力。

6.1.3 主机安全

身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制应符合 GB/T 22239—2008 中 6.1.3 的要求。

6.1.4 应用安全

6.1.4.1 基本要求

身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制应符合 GB/T 22239—2008 中 6.1.4 的要求。

6.1.4.2 身份鉴别(S2)

身份鉴别除基本要求外，还应满足：

a) 建立感知终端的标识管理机制；

b) 对来自于感知终端的信息采取先验证信息源再处理的机制。

6.1.4.3 感知终端软件更新(A2)

感知终端软件更新应满足以下要求：

a) 具有适应公安物联网应用业务扩展和安全加固的更新机制；

b) 具有回退机制，保证未正常更新的感知终端能恢复到更新前的状态。

6.1.4.4 感知设备访问控制(S2)

感知设备访问控制应满足以下要求：

a) 设置感知层入网访问控制；

b) 进行远程软件配置时，提供访问控制机制。

6.1.5 数据安全及备份恢复

6.1.5.1 基本要求

数据完整性、数据保密性、备份和恢复应符合 GB/T 22239—2008 中 6.1.5 的要求。

6.1.5.2 数据完整性(S2)

数据完整性除基本要求外，还应能够检测到感知终端生存信息、鉴别信息和隐私性数据在传输过程

中完整性受到破坏。

6.1.5.3 数据可用性(A2)

应保证感知设备之间通信数据的可用性。

6.1.5.4 敏感数据加密(G2)

敏感数据加密应满足以下要求：

a) 采集敏感信息的感知设备对本地存储数据进行加密；

b) 采集敏感信息的感知设备对上传的数据进行加密。

6.1.5.5 用户隐私安全(A2)

用户隐私安全应满足以下要求：

a) 保护感知终端所存储的用户隐私不被泄露；

b) 保证公安物联网络通信网络用户身份的隐私。

6.1.5.6 数据保密性(S2)

数据保密性除基本要求外，还应采用加密或其他有效措施实现鉴别信息和隐私性数据存储保密性。

6.2 管理要求

6.2.1 安全管理制度

管理制度、制定和发布、评审和修订应符合 GB/T 22239—2008 中 6.2.1 的要求。

6.2.2 安全管理机构

岗位设置、人员配备、授权和审批、沟通和合作、审核和检查应符合 GB/T 22239—2008 中 6.2.2 的要求。

6.2.3 人员安全管理

人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理应符合 GB/T 22239—2008 中 6.2.3 的要求。

6.2.4 系统建设管理

6.2.4.1 基本要求

系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择应符合 GB/T 22239—2008 中 6.2.4 的要求。

6.2.4.2 产品采购和使用(G2)

产品采购和使用除基本要求外，感知设备还应符合国家的有关规定。

6.2.4.3 自行研发感知设备(G2)

自行研发感知设备应满足以下要求：

a) 主要部件参数满足系统功能需求；

b) 研发环境与实际运行环境物理分开；

c) 提供感知设备软、硬件设计的相关文档，并由专人负责保管；

d) 制定感知设备的软、硬件研发管理制度，明确说明研发过程的控制方法和人员行为准则。

6.2.4.4 外包研发感知设备(G2)

外包研发感知设备应满足以下要求：

a) 根据研发需求检测感知设备软、硬件质量；

b) 在软件安装之前检测软件包中可能存在的恶意代码；

c) 要求研发单位提供软、硬件设计的相关文档和使用指南；

d) 根据研发单位提供的硬件设计图审查实物与设计是否一致。

6.2.5 系统运维管理

6.2.5.1 基本要求

环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理应符合 GB/T 22239—2008 中 6.2.5 的要求。

6.2.5.2 环境管理(G2)

环境管理除基本要求外，还应满足以下要求：

a) 定期巡视感知终端、物联网网关的部署环境，对可能影响感知终端、物联网网关正常工作的环境异常进行记录和维护；

b) 制定感知终端、物联网网关入库、存储、部署、携带、维修、丢失和报废等管理制度，并进行全程管理；

c) 加强对感知终端、物联网网关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；

d) 记录感知终端、物联网网关的外观、电量、指示灯等状态信息，对物联网网关进行现场维护。

6.2.5.3 备份与恢复管理(G2)

备份与恢复管理除基本要求外，还应满足：

a) 规定感知终端、物联网网关备份信息的备份方式、备份频度、存储介质、保存期等；

b) 根据感知终端、物联网网关数据的重要性及其对系统运行的影响，制定感知终端、物联网网关数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

7 第三级要求

7.1 技术要求

7.1.1 物理安全

7.1.1.1 基本要求

物理位置的选择、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、电磁防护应符合 GB/T 22239—2008 中 7.1.1 的要求。

7.1.1.2 物理位置的选择(G3)

物理位置的选择除基本要求外,公安物联网户外设备应满足以下要求:

a) 选择部署在不易被破坏、被移除的位置;

b) 部署在能定期巡查的位置。

7.1.1.3 防盗窃和防破坏(G3)

防盗窃和防破坏除基本要求外,公安物联网户外设备还应采取专用工具且不易拆卸的方式安装。

7.1.1.4 感知终端的物理安全(G3)

感知终端的物理安全应满足以下要求:

a) 所处的物理环境不对感知终端造成物理破坏;

b) 能准确反映所处的物理环境状态;

c) 关键感知终端所处的物理环境避免信号干扰。

7.1.1.5 物联网网关的物理安全(G3)

物联网网关的物理安全应满足以下要求:

a) 所在物理环境具备防火、防静电、防潮和防水的能力;

b) 固定主要部件,并设置明显的不易除去的标记;

c) 关键物联网网关所在物理环境保证其具有良好的信号收发能力。

7.1.1.6 防雷击(G3)

防雷击除基本要求外,公安物联网户外设备还应设置必要的避雷或防雷措施。

7.1.1.7 防水和防潮(G3)

防水和防潮除基本要求外,公安物联网户外设备还应设置必要的防水和防潮措施。

7.1.1.8 防静电(G3)

防静电除基本要求外,公安物联网户外设备还应设置防静电措施。

7.1.1.9 电力供应(A3)

电力供应除基本要求外,还应满足:

a) 公安物联网户外有源设备提供必要的电池续电能力;

b) 公安物联网户外有源设备电力不足时应提供断电报警功能;

c) 关键物联网网关具有持久的、稳定的电力供应能力。

7.1.1.10 电磁防护(S3)

电磁防护除基本要求外,公安物联网户外设备还应采取防电磁干扰等措施。

7.1.2 网络安全

7.1.2.1 基本要求

结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护应符合

GB/T 22239—2008 中 7.1.2 的要求。

7.1.2.2 结构安全(G3)

结构安全除基本要求外,还应确保感知设备的信息和服务可以提供给合法用户。

7.1.2.3 访问控制(S3)

访问控制除基本要求外,还应满足:

a) 设置感知终端入网访问控制;
b) 远程配置感知终端、物联网网关的软件应用时,进行访问控制;
c) 对感知终端接入网络资源设置访问控制机制;
d) 防止感知终端和感知层资源被非法访问和非法使用;
e) 只有经过授权的软件应用才能被下载到物联网终端、物联网网关上;
f) 只有合法用户可以通过外部接口提交关于物联网终端、物联网网关的信息更改请求。

7.1.2.4 感知设备防护(A3)

感知设备防护应满足以下要求:

a) 采取措施防止感知设备被破坏和篡改;
b) 对有卡的设备,采取措施防止通用集成电路卡或者用户识别卡非法拔出或替换;
c) 对无卡的设备,采取措施防止信任状态被非法复制或者篡改。

7.1.2.5 设备标识(S3)

设备标识应满足以下要求:

a) 对感知设备建立系统内唯一的标识信息;
b) 具有对连接的感知设备进行身份标识与鉴别的能力;
c) 具有识别发送非法或伪造数据感知设备的能力;
d) 具有识别重放历史数据的感知设备的能力。

7.1.2.6 感知设备认证(S3)

感知设备认证应满足以下要求:

a) 对感知设备建立注册和认证机制;
b) 感知设备需在系统注册和认证之后接入网络中;
c) 依据感知设备唯一标识建立系统接入预注册机制,完善对感知设备的资产管理;
d) 在感知设备和服务器之间采取双向身份认证机制。

7.1.2.7 组认证(S3)

应采取措施使物联网应用服务器对感知终端构成的组提供组认证的能力。

7.1.2.8 数据源认证(S3)

数据源认证应满足以下要求:

a) 信息来源于正确的物联网网关;
b) 物联网网关没有被恶意注入虚假信息。

7.1.2.9 异构网接入(S3)

异构网接入应满足以下要求:

a） 对异构网络的接入进行安全检测；

b） 具有拒绝恶意节点的接入能力；

c） 确保异构网接入时转发数据的完整性和保密性；

d） 根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段。

7.1.2.10 终端位置隐私保护（G3）

应具有感知终端物理位置和网络地址隐私保护的能力。

7.1.3 主机安全

身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制应符合GB/T 22239—2008中7.1.3的要求。

7.1.4 应用安全

7.1.4.1 基本要求

身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制应符合GB/T 22239—2008中7.1.4的要求。

7.1.4.2 身份鉴别（S3）

身份鉴别除基本要求外，还应满足：

a） 建立感知终端的标识管理机制，对来自于感知终端的信息，先采取基于密钥鉴别的方式验证信息源后再处理的机制；

b） 对来自于感知终端的信息采取先验证信息源再处理的机制；

c） 公安物联网业务用户的身份鉴别能防范身份鉴别中的重放攻击。

7.1.4.3 感知终端软件更新（A3）

感知终端软件更新应满足以下要求：

a） 具有适应公安物联网应用业务扩展和安全加固的更新机制；

b） 具有回退机制，保证未正常更新的感知终端能恢复到更新前的状态；

c） 软件更新包提供源验证和完整性保证机制；

d） 软件更新过程具有分组和分时段更新机制。

7.1.4.4 感知设备访问控制（S3）

感知设备访问控制应满足以下要求：

a） 设置感知层入网访问控制；

b） 进行远程软件配置时，提供访问控制机制。

7.1.4.5 安全审计（G3）

安全审计除基本要求外，还应对公安物联网中的非法业务进行告警，告警信息中至少包括非法业务的上线时间、位置、状态等内容。

7.1.4.6 业务管理（A3）

业务管理应满足以下要求：

a) 建立业务管理和生命周期管理机制；
b) 建立完整的公安物联网业务注册、审核和发布机制。

7.1.5 数据安全及备份恢复

7.1.5.1 基本要求

数据完整性、数据保密性、备份和恢复应符合 GB/T 22239—2008 中 7.1.5 的要求。

7.1.5.2 数据完整性(S3)

数据完整性除基本要求外，还应能够检测到感知终端生存信息、系统管理数据、鉴别信息、隐私性数据和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

7.1.5.3 数据可用性(A3)

数据可用性应满足以下要求：
a) 保证感知设备之间通信数据的可用性；
b) 提供关键物联网网关和通信线路冗余；
c) 支持网络传输质量保证功能。

7.1.5.4 敏感数据加密(G3)

采集敏感信息的感知设备，敏感数据加密应满足以下要求：
a) 对本地存储数据进行加密；
b) 对上传的数据进行加密。

7.1.5.5 用户隐私安全(A3)

用户隐私安全应满足以下要求：
a) 保护感知终端所存储的用户隐私不被泄露；
b) 保证公安物联网络通信网络用户身份的隐私。

7.1.5.6 数据保密性(S3)

数据保密性除基本要求外，还应采用加密或其他有效措施实现鉴别信息和隐私性数据等敏感数据存储保密性。

7.2 管理要求

7.2.1 安全管理制度

管理制度、制定和发布、评审和修订应符合 GB/T 22239—2008 中 7.2.1 的要求。

7.2.2 安全管理机构

岗位设置、人员配备、授权和审批、沟通和合作、审核和检查应符合 GB/T 22239—2008 中 7.2.2 的要求。

7.2.3 人员安全管理

人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理应符合 GB/T 22239—2008 中 7.2.3 的要求。

7.2.4 系统建设管理

7.2.4.1 基本要求

系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择应符合 GB/T 22239—2008 中 7.2.4 的要求。

7.2.4.2 产品采购和使用(G3)

产品采购和使用除基本要求外，感知设备还应符合国家的有关规定。

7.2.4.3 自行研发感知设备(G3)

自行研发感知设备应满足以下要求：

a) 主要部件参数满足系统功能需求；
b) 研发环境与实际运行环境物理分开；
c) 提供感知设备软、硬件设计的相关文档，并由专人负责保管；
d) 制定感知设备的软、硬件研发管理制度，明确说明研发过程的控制方法和人员行为准则；
e) 制定感知设备自行研发安全规范；
f) 确保对感知设备软、硬件设计资源库的修改、更新、发布进行授权和批准。

7.2.4.4 外包研发感知设备(G3)

外包研发感知设备应满足以下要求：

a) 根据研发需求检测感知设备软、硬件质量；
b) 要求研发单位提供软件源代码，并审查软件中可能存在的后门；
c) 要求研发单位提供硬件设计图，并审查硬件设计中可能存在的后门；
d) 根据研发单位提供的硬件设计图审查实物与设计是否一致。

7.2.5 系统运维管理

7.2.5.1 基本要求

环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置和应急预案管理应符合 GB/T 22239—2008 中 7.2.5 的要求。

7.2.5.2 环境管理(G3)

环境管理除基本要求外，还应满足以下要求：

a) 定期巡视感知终端、物联网网关的部署环境，对可能影响感知终端、物联网网关正常工作的环境异常进行记录和维护；
b) 制定感知终端、物联网网关入库、存储、部署、携带、维修、丢失和报废等管理制度，并进行全程管理；
c) 加强对感知终端、物联网网关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；
d) 记录感知终端、物联网网关的外观、电量、指示灯等状态信息，对物联网网关进行现场维护；
e) 建立针对感知终端、物联网网关部署环境的评估制度，编写可操作评估方法，并由专人完成评估。

7.2.5.3 备份与恢复管理(G3)

备份与恢复管理除基本要求外,还应满足:

a) 规定感知终端、物联网网关备份信息的备份方式、备份频度、存储介质、保存期等;

b) 根据感知终端、物联网网关数据的重要性及其对系统运行的影响,制定感知终端、物联网网关数据的备份策略和恢复策略,备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法;

c) 建立控制数据备份和恢复过程的程序,对备份过程进行记录,所有文件和记录妥善保存;

d) 定期执行恢复程序,检查和测试备份介质的有效性,确保在恢复程序规定的时间内完成备份的恢复;

e) 建立备份与恢复管理相关的安全管理制度,对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。

7.2.5.4 监控管理和安全管理中心(G3)

监控管理和安全管理中心除基本要求外,还应满足:

a) 对感知终端、物联网网关和相关软件的运行状况、网络流量、用户行为等进行监测和报警,形成记录并妥善保存;

b) 组织相关人员定期对监测和报警记录进行分析、评审,发现可疑行为,形成分析报告,并采取必要的应对措施;

c) 安全管理中心对感知设备状态、补丁升级、安全审计等安全相关事项进行集中管理。

8 第四级要求

8.1 技术要求

8.1.1 物理安全

8.1.1.1 基本要求

物理位置的选择、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、电磁防护应符合 GB/T 22239—2008 中 8.1.1 的要求。

8.1.1.2 物理位置的选择(G4)

物理位置的选择除基本要求外,公安物联网户外设备应满足以下要求:

a) 选择部署在不易被破坏、被移除的位置;

b) 部署在能定期巡查的位置。

8.1.1.3 防盗窃和防破坏(G4)

防盗窃和防破坏除基本要求外,公安物联网户外设备还应采取专用工具且不易拆卸的方式安装。

8.1.1.4 感知终端的物理安全(G4)

感知终端的物理安全应满足以下要求:

a) 所处的物理环境不对感知终端造成物理破坏;

b) 能准确反映所处的物理环境状态;

c) 所处的物理环境避免信号干扰。

8.1.1.5 物联网网关的物理安全(G4)

物联网网关的物理安全应满足以下要求：

a) 所在物理环境具备防火、防静电、防潮和防水的能力；

b) 固定主要部件，并设置明显的不易除去的标记；

c) 公安物联网网关所在物理环境保证其具有良好的信号收发能力。

8.1.1.6 防雷击(G4)

防雷击除基本要求外，公安物联网户外设备还应设置必要的避雷或防雷措施。

8.1.1.7 防水和防潮(G4)

防水和防潮除基本要求外，公安物联网户外设备还应设置必要的防水和防潮措施。

8.1.1.8 防静电(G4)

防静电除基本要求外，公安物联网户外设备还应设置防静电措施。

8.1.1.9 电力供应(A4)

电力供应除基本要求外，还应满足：

a) 公安物联网户外有源设备提供必要的电池续电能力；

b) 公安物联网户外有源设备电力不足时应提供断电报警功能；

c) 公安物联网网关具有持久的，稳定的电力供应能力。

8.1.1.10 电磁防护(S4)

电磁防护除基本要求外，公安物联网户外设备还应采取防电磁干扰等措施。

8.1.2 网络安全

8.1.2.1 基本要求

结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护应符合GB/T 22239—2008 中 8.1.2 的要求。

8.1.2.2 结构安全(G4)

结构安全除基本要求外，还应满足：

a) 感知网络的信息和服务在任何时间提供给合法用户；

b) 保证接收到数据的实效性，确保没有恶意感知终端重放信息。

8.1.2.3 访问控制(S4)

访问控制除基本要求外，还应满足：

a) 设置感知终端和物联网网关入网访问控制；

b) 远程配置感知终端、物联网网关的软件应用时，进行访问控制；

c) 防止感知终端和感知层资源被非法访问和非法使用；

d) 只有经过授权的软件应用才能被下载到物联网终端、物联网网关上；

e) 由授权主体配置访问控制策略，限制默认账户的访问权限；

f) 授予不同账户为完成各自承担任务所需的最小权限，并形成相互制约关系。

8.1.2.4 感知设备防护(A4)

感知设备防护应满足以下要求：

a) 采取措施防止感知设备被破坏和篡改；

b) 对有卡的设备，采取措施防止通用集成电路卡或者用户识别卡非法拔出或替换；

c) 对无卡的设备，采取措施防止信任状态被非法复制或者篡改。

8.1.2.5 设备标识(S4)

设备标识应满足以下要求：

a) 对感知设备建立系统内唯一的标识信息；

b) 具有对连接的感知设备进行身份标识与鉴别的能力；

c) 具备过滤非法感知设备和伪造感知设备所发送的数据的能力；

d) 具备防止非法感知设备重放合法感知设备的历史数据的能力。

8.1.2.6 感知设备认证(S4)

感知设备认证应满足以下要求：

a) 对感知设备建立注册和认证机制；

b) 感知设备需在系统注册和认证之后才可以接入网络中；

c) 依据感知设备唯一标识建立系统接入预注册机制，完善对感知设备的资产管理；

d) 在感知设备和服务器之间采取双向身份认证机制，通过系统内唯一标识和可信鉴别组件的绑定，实现感知设备可信接入和服务器可信访问。

8.1.2.7 组认证(S4)

应采取措施使物联网应用服务器对感知终端构成的组提供组认证的能力。

8.1.2.8 数据源认证(S4)

数据源认证应满足以下要求：

a) 信息来源于正确的物联网网关；

b) 物联网网关没有被恶意注入虚假信息。

8.1.2.9 异构网接入(S4)

异构网接入应满足以下要求：

a) 对异构网络的接入进行安全检测；

b) 具有拒绝恶意节点的接入能力；

c) 确保异构网接入时转发数据的完整性和保密性；

d) 根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段；

e) 对重要通信提供专用通信协议或安全通信协议服务。

8.1.2.10 网络设备防护(G4)

网络设备防护除基本要求外，还应满足网络传输质量应满足物联网应用单位对感知数据设备(含传感器网络)的完整性、连续性和实时性的需求。

8.1.2.11 终端位置隐私保护(G4)

应具有感知终端物理位置和网络地址隐私保护的能力。

8.1.2.12 业务认证(S4)

应采取措施对感知终端与物联网应用服务器之间进行业务认证。

8.1.3 主机安全

身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制应符合 GB/T 22239—2008 中 8.1.3 的要求。

8.1.4 应用安全

8.1.4.1 基本要求

身份鉴别、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制应符合 GB/T 22239—2008 中 8.1.4 的要求。

8.1.4.2 身份鉴别(S4)

身份鉴别除基本要求外,还应满足:

a) 建立感知终端的标识管理机制,对来自于感知终端的信息,应先采取基于密钥的双向鉴别方式验证信息源后再处理;
b) 对来自于感知终端的信息采取先验证信息源再处理的机制;
c) 公安物联网业务用户身份鉴别应能防范身份鉴别中的重放攻击。

8.1.4.3 访问控制(S4)

访问控制除基本要求外,还应满足:

a) 用户使用业务前经过业务授权;
b) 防止假冒用户使用未授权的业务或者合法用户使用未定制的业务。

8.1.4.4 感知终端软件更新(A4)

感知终端软件更新应满足以下要求:

a) 具有适应公安物联网应用业务扩展和安全加固的更新机制;
b) 具有回退机制,保证未正常更新的感知终端能恢复到更新前的状态;
c) 软件更新包应提供源验证和完整性保证机制;
d) 软件更新过程应具有分组和分时段更新机制。

8.1.4.5 感知设备访问控制(S4)

感知设备访问控制应满足以下要求:

a) 设置感知层入网访问控制;
b) 进行远程软件配置时,提供访问控制机制。

8.1.4.6 安全审计(G4)

安全审计除基本要求外,还应对公安物联网中的非法业务进行告警,告警信息中至少包括非法业务

的上线时间、位置、状态等内容。

8.1.4.7 业务管理(A4)

业务管理应满足以下要求：

a) 建立业务管理和生命周期管理机制；

b) 建立完整的公安物联网业务注册、审核和发布机制；

c) 建立非法业务接入监控和通报机制。

8.1.5 数据安全及备份恢复

8.1.5.1 基本要求

数据完整性、数据保密性、备份和恢复应符合 GB/T 22239—2008 中 8.1.5 的要求。

8.1.5.2 数据完整性(S4)

数据完整性除基本要求外，还应能够检测到感知终端生存信息、系统管理数据、鉴别信息、隐私性数据和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

8.1.5.3 数据可用性(A4)

数据可用性应满足以下要求：

a) 保证感知设备之间通信数据的可用性；

b) 提供关键物联网网关和通信线路冗余；

c) 支持网络传输质量保证功能。

8.1.5.4 敏感数据加密(G4)

采集敏感信息的感知设备，敏感数据加密应满足以下要求：

a) 对本地存储数据进行加密；

b) 对上传的数据进行加密。

8.1.5.5 用户隐私安全(A4)

用户隐私安全应满足以下要求：

a) 保护感知终端所存储的用户隐私不被泄露；

b) 保证公安物联网络通信网络用户身份的隐私。

8.1.5.6 数据保密性(S4)

数据保密性除基本要求外，还应采用加密或其他有效措施实现鉴别信息和隐私性数据等敏感数据存储保密性。

8.2 管理要求

8.2.1 安全管理制度

管理制度、制定和发布、评审和修订应符合 GB/T 22239—2008 中 8.2.1 的要求。

8.2.2 安全管理机构

岗位设置、人员配备、授权和审批、沟通和合作、审核和检查应符合 GB/T 22239—2008 中 8.2.2 的

要求。

8.2.3 人员安全管理

人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理应符合 GB/T 22239—2008 中 8.2.3 的要求。

8.2.4 系统建设管理

8.2.4.1 基本要求

系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择应符合 GB/T 22239—2008 中 8.2.4 的要求。

8.2.4.2 产品采购和使用(G4)

产品采购和使用除基本要求外,感知设备还应符合国家的有关规定。

8.2.4.3 自行研发感知设备(G4)

自行研发感知设备应满足以下要求:

a) 主要部件参数满足系统功能需求;
b) 研发环境与实际运行环境物理分开;
c) 提供感知设备软、硬件设计的相关文档,并由专人负责保管;
d) 制定感知设备的软、硬件研发管理制度,明确说明研发过程的控制方法和人员行为准则;
e) 制定感知设备自行研发安全规范;
f) 确保对感知设备软、硬件设计资源库的修改、更新、发布进行授权和批准。

8.2.4.4 外包研发感知设备(G4)

外包研发感知设备应满足以下要求:

a) 根据研发需求检测感知设备软、硬件质量;
b) 要求研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;
c) 要求研发单位提供硬件设计图,并审查硬件设计中可能存在的后门和隐蔽信道;
d) 应根据研发单位提供的硬件设计图审查实物与设计是否一致。

8.2.5 系统运维管理

8.2.5.1 基本要求

环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理应符合 GB/T 22239—2008 中 8.2.5 的要求。

8.2.5.2 环境管理(G4)

环境管理除基本要求外,还应满环境管理除基本要求外,还应满足以下要求:

a) 定期巡视感知终端、物联网网关的部署环境,对可能影响感知终端、物联网网关正常工作的环境异常进行记录和维护;
b) 制定感知终端、物联网网关入库、存储、部署、携带、维修、丢失和报废等管理制度,并进行全程管理;

c) 加强对感知终端、物联网网关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立即交还相关检查工具和检查维护记录等；
d) 指定部门负责感知终端、物联网网关的部署环境的安全，并配备安全管理人员记录感知终端、物联网网关的状态，对物联网网关进行现场维护；
e) 建立针对感知终端、物联网网关部署环境的评估制度，编写可操作评估方法，并由专人完成评估。

8.2.5.3 备份与恢复管理(G4)

备份与恢复管理除基本要求外，还应满足：

a) 规定感知终端、物联网网关备份信息的备份方式、备份频度、存储介质、保存期等；
b) 根据感知终端、物联网网关数据的重要性及其对系统运行的影响，制定感知终端、物联网网关数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法；
c) 建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；
d) 定期执行恢复程序，检查和测试备份介质的有效性，确保在恢复程序规定的时间内完成备份的恢复；
e) 建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。

8.2.5.4 监控管理和安全管理中心(G4)

监控管理和安全管理中心除基本要求外，还应满足：

a) 对感知终端、物联网网关和相关软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
b) 组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
c) 安全管理中心应对感知设备状态、补丁升级、安全审计等安全相关事项进行集中管理。

中 华 人 民 共 和 国
国 家 标 准
公安物联网系统信息安全等级保护要求
GB/T 35317—2017
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017 年 12 月第一版
*
书号:155066·1-58841

GB/T 35317-2017