b) 测评对象:服务水平协议或服务合同。
c) 测评实施:应核查服务水平协议或服务合同是否明确服务合约到期时,云服务商完整提供云服务客户数据,并承诺相关数据在云计算平台上清除。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.6.1.5 测评单元(L3-CMS2-05)

该测评单元包括以下要求:
a) 测评指标:应与选定的云服务商签署保密协议,要求其不得泄露云服务客户数据。
b) 测评对象:保密协议或服务合同。
c) 测评实施:应核查保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据的规定。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.6.2 供应链管理

8.2.6.2.1 测评单元(L3-CMS2-07)

该测评单元包括以下要求:
a) 测评指标:应确保供应商的选择符合国家有关规定。
b) 测评对象:记录表单类文档。
c) 测评实施:应核查云服务商的选择是否符合国家的有关规定。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.6.2.2 测评单元(L3-CMS2-08)

该测评单元包括以下要求:
a) 测评指标:应将供应链安全事件信息或威胁信息及时传达到云服务客户。
b) 测评对象:供应链安全事件报告或威胁报告。
c) 测评实施:应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户,报告是否明确相关事件信息或威胁信息。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.6.2.3 测评单元(L3-CMS2-09)

该测评单元包括以下要求:
a) 测评指标:应将供应商的重要变更及时传达到云服务客户,并评估变更带来的安全风险,采取措施对风险进行控制。
b) 测评对象:供应商重要变更记录、安全风险评估报告和风险预案。
c) 测评实施:应核查供应商的重要变更是否及时传达到云服务客户,是否对每次供应商的重要变更都进行风险评估并采取控制措施。
d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.7 安全运维管理

8.2.7.1 云计算环境管理

8.2.7.1.1 测评单元(L3-MMS2-01)

该测评单元包括以下要求：

a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。

c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.3 移动互联安全测评扩展要求

8.3.1 安全物理环境

8.3.1.1 无线接入点的物理位置

8.3.1.1.1 测评单元(L3-PES3-01)

该测评单元包括以下要求：

a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

b) 测评对象：无线接入设备。

c) 测评实施包括以下内容：

1) 应核查物理位置与无线信号的覆盖范围是否合理；

2) 应测试验证无线信号是否可以避免电磁干扰。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 安全区域边界

8.3.2.1 边界防护

8.3.2.1.1 测评单元(L3-ABS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

b) 测评对象：无线接入网关设备。

c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.2 访问控制

8.3.2.2.1 测评单元(L3-ABS3-02)

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3 入侵防范

8.3.2.3.1 测评单元(L3-ABS3-03)

该测评单元包括以下要求：

a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够检测非授权无线接入设备和移动终端的接入行为；
   2) 应测试验证是否能够检测非授权无线接入设备和移动终端的接入行为。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2.3.2 测评单元(L3-ABS3-04)

该测评单元包括以下要求：

a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。
b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测；
   2) 应核查规则库版本是否及时更新。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2.3.3 测评单元(L3-ABS3-05)

该测评单元包括以下要求：

a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
b) 测评对象：无线接入设备或相关组件。
c) 测评实施：应核查是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3.4 测评单元(L3-ABS3-06)

该测评单元包括以下要求：

a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
b) 测评对象：无线接入设备和无线接入网关设备。
c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3.5 测评单元(L3-ABS3-07)

该测评单元包括以下要求：
a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥。
b) 测评对象：无线接入设备。
c) 测评实施：应核查是否分别使用了不同的鉴别密钥。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3.6 测评单元(L3-ABS3-08)

该测评单元包括以下要求：
a) 测评指标：应能够阻断非授权无线接入设备或非授权移动终端。
b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否能够阻断非授权无线接入设备或非授权移动终端接入；
   2) 应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3 安全计算环境

8.3.3.1 移动终端管控

8.3.3.1.1 测评单元(L3-CES3-01)

该测评单元包括以下要求：
a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施：应核查移动终端是否安装、注册并运行移动终端客户端软件。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.1.2 测评单元(L3-CES3-02)

该测评单元包括以下要求：
a) 测评指标：移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
b) 测评对象：移动终端和移动终端管理系统。
c) 测评实施包括以下内容：

1） 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略；

2） 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。

d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3.2 移动应用管控

8.3.3.2.1 测评单元（L3-CES3-03）

该测评单元包括以下要求：

a） 测评指标：应具有选择应用软件安装、运行的功能。

b） 测评对象：移动终端管理客户端。

c） 测评实施：应核查是否具有选择应用软件安装、运行的功能。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.2.2 测评单元（L3-CES3-04）

该测评单元包括以下要求：

a） 测评指标：应只允许指定证书签名的应用软件安装和运行。

b） 测评对象：移动终端管理客户端。

c） 测评实施：应核查全部移动应用是否由指定证书签名。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.2.3 测评单元（L3-CES3-05）

该测评单元包括以下要求：

a） 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

b） 测评对象：移动终端管理客户端。

c） 测评实施包括以下内容：

1） 应核查是否具有软件白名单功能；

2） 应测试验证白名单功能是否能够控制应用软件安装、运行。

d） 单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.4 安全建设管理

8.3.4.1 移动应用软件采购

8.3.4.1.1 测评单元（L3-CMS3-01）

该测评单元包括以下要求：

a） 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b） 测评对象：移动终端。

c） 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.1.2 测评单元（L3-CMS3-02）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件由指定的开发者开发。

b) 测评对象：移动终端。

c) 测评实施：应核查移动应用软件是否由指定的开发者开发。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.2 移动应用软件开发

8.3.4.2.1 测评单元（L3-CMS3-03）

该测评单元包括以下要求：

a) 测评指标：应对移动业务应用软件开发者进行资格审查。

b) 测评对象：系统建设负责人。

c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.2.2 测评单元（L3-CMS3-04）

该测评单元包括以下要求：

a) 测评指标：应保证开发移动业务应用软件的签名证书合法性。

b) 测评对象：软件的签名证书。

c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.5 安全运维管理

8.3.5.1 配置管理

8.3.5.1.1 测评单元（L3-MMS3-01）

该测评单元包括以下要求：

a) 测评指标：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

b) 测评对象：记录表单类文档、移动终端管理系统或相关组件。

c) 测评实施：应核查是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4 物联网安全测评扩展要求

8.4.1 安全物理环境

8.4.1.1 感知节点设备物理防护

8.4.1.1.1 测评单元(L3-PES4-01)

该测评单元包括以下要求：

a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动。

b) 测评对象：感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；

2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.2 测评单元(L3-PES4-02)

该测评单元包括以下要求：

a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

b) 测评对象：感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；

2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.3 测评单元(L3-PES4-03)

该测评单元包括以下要求：

a) 测评指标：感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等。

b) 测评对象：感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容：

1) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致；

2) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.4 测评单元(L3-PES4-04)

该测评单元包括以下要求：

a) 测评指标:关键感知节点设备应具有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应能力)。
b) 测评对象:关键感知节点设备的供电设备(关键网关节点设备的供电设备)和设计或验收文档。
c) 测评实施包括以下内容:
   1) 应核查关键感知节点设备(关键网关节点设备)电力供应设计或验收文档是否标明电力供应要求,其中是否明确保障关键感知节点设备长时间工作的电力供应措施(关键网关节点设备持久稳定的电力供应措施);
   2) 应核查是否具有相关电力供应措施的运行维护记录,是否与电力供应设计一致。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.4.2 安全区域边界

8.4.2.1 接入控制

8.4.2.1.1 测评单元(L3-ABS4-01)

该测评单元包括以下要求:
a) 测评指标:应保证只有授权的感知节点可以接入。
b) 测评对象:感知节点设备和设计文档。
c) 测评实施包括以下内容:
   1) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述;
   2) 应对边界和感知层网络进行渗透测试,测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.4.2.2 入侵防范

8.4.2.2.1 测评单元(L3-ABS4-02)

该测评单元包括以下要求:
a) 测评指标:应能够限制与感知节点通信的目标地址,以避免对陌生地址的攻击行为。
b) 测评对象:感知节点设备和设计文档。
c) 测评实施包括以下内容:
   1) 应核查感知层安全设计文档,是否有对感知节点通信目标地址的控制措施说明;
   2) 应核查感知节点设备,是否配置了对感知节点通信目标地址的控制措施,相关参数配置是否符合设计要求;
   3) 应对感知节点设备进行渗透测试,测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
d) 单元判定:如果 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.4.2.2.2 测评单元(L3-ABS4-03)

该测评单元包括以下要求:

a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。
b) 测评对象：网关节点设备和设计文档。
c) 测评实施包括以下内容：
   1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；
   2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
   3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3 安全计算环境

8.4.3.1 感知节点设备安全

8.4.3.1.1 测评单元(L3-CES4-01)

该测评单元包括以下要求：

a) 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。
b) 测评对象：感知节点设备。
c) 测评实施包括以下内容：
   1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；
   2) 应通过试图接入和控制传感网访问未授权的资源，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.1.2 测评单元(L3-CES4-02)

该测评单元包括以下要求：

a) 测评指标：应具有对其连接的网关节点设备(包括读卡器)进行身份标识和鉴别的能力。
b) 测评对象：网关节点设备(包括读卡器)。
c) 测评实施包括以下内容：
   1) 应核查是否对连接的网关节点设备(包括读卡器)进行身份标识与鉴别，是否配置了符合安全策略的参数；
   2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.1.3 测评单元(L3-CES4-03)

该测评单元包括以下要求：

a) 测评指标：应具有对其连接的其他感知节点设备(包括路由节点)进行身份标识和鉴别的能力。
b) 测评对象：其他感知节点设备(包括路由节点)。

c) 测评实施包括以下内容：

1) 应核查是否对连接的其他感知节点设备(包括路由节点)设备进行身份标识与鉴别，是否配置了符合安全策略的参数；

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2 网关节点设备安全

8.4.3.2.1 测评单元(L3-CES4-04)

该测评单元包括以下要求：

a) 测评指标：应设置最大并发连接数。

b) 测评对象：网关节点设备。

c) 测评实施：应核查网关节点设备是否配置了最大并发连接数参数。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4.3.2.2 测评单元(L3-CES4-05)

该测评单元包括以下要求：

a) 测评指标：应具备对合法连接设备(包括终端节点、路由节点、数据处理中心)进行标识和鉴别的能力。

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查网关节点设备是否能够对连接设备(包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能；

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.3 测评单元(L3-CES4-06)

该测评单元包括以下要求：

a) 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力。

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查是否具备过滤非法节点和伪造节点发送的数据的功能；

2) 应测试验证是否能够过滤非法节点和伪造节点发送的数据。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.4 测评单元(L3-CES4-07)

该测评单元包括以下要求：

a) 测评指标：授权用户应能够在设备使用过程中对关键密钥进行在线更新。

b) 测评对象:感知节点设备。
c) 测评实施:应核查感知节点设备是否对其关键密钥进行在线更新。
d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.4.3.2.5 测评单元(L3-CES4-08)

该测评单元包括以下要求:

a) 测评指标:授权用户应能够在设备使用过程中对关键配置参数进行在线更新。
b) 测评对象:感知节点设备。
c) 测评实施:应核查是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。
d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.4.3.3 抗数据重放

8.4.3.3.1 测评单元(L3-CES4-09)

该测评单元包括以下要求:

a) 测评指标:应能够鉴别数据的新鲜性,避免历史数据的重放攻击。
b) 测评对象:感知节点设备。
c) 测评实施包括以下内容:
   1) 应核查感知节点设备鉴别数据新鲜性的措施,是否能够避免历史数据重放;
   2) 应将感知节点设备历史数据进行重放测试,验证其保护措施是否生效。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.4.3.3.2 测评单元(L3-CES4-10)

该测评单元包括以下要求:

a) 测评指标:应能够鉴别历史数据的非法修改,避免数据的修改重放攻击。
b) 测评对象:感知节点设备。
c) 测评实施包括以下内容:
   1) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施,在检测到被修改时是否能采取必要的恢复措施;
   2) 应测试验证是否能够避免数据的修改重放攻击。
d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.4.3.4 数据融合处理

8.4.3.4.1 测评单元(L3-CES4-11)

该测评单元包括以下要求:

a) 测评指标:应对来自传感网的数据进行数据融合处理,使不同种类的数据可以在同一个平台被使用。
b) 测评对象:物联网应用系统。
c) 测评实施包括以下内容:

1) 应核查是否提供对来自传感网的数据进行数据融合处理的功能；
2) 应测试验证数据融合处理功能是否能够处理不同种类的数据。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4 安全运维管理

8.4.4.1 感知节点管理

8.4.4.1.1 测评单元(L3-MMS4-01)

该测评单元包括以下要求：

a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。
b) 测评对象：维护记录。
c) 测评实施包括以下内容：
   1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；
   2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4.1.2 测评单元(L3-MMS4-02)

该测评单元包括以下要求：

a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
b) 测评对象：感知节点和网关节点设备安全管理文档。
c) 测评实施：应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4.4.1.3 测评单元(L3-MMS4-03)

该测评单元包括以下要求：

a) 测评指标：应加强对感知节点设备、网关节点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。
b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度。
c) 测评实施：
   1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容；
   2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5 工业控制系统安全测评扩展要求

8.5.1 安全物理环境

8.5.1.1 室外控制设备物理防护

8.5.1.1.1 测评单元(L3-PES5-01)

该测评单元包括以下要求：

a) 测评指标：室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

1) 应核查是否放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；

2) 应核查箱体或装置是否具有透风、散热、防盗、防雨和防火能力等。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.1.1.2 测评单元(L3-PES5-02)

该测评单元包括以下要求：

a) 测评指标：室外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及检修，保证设备正常运行。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

1) 应核查放置位置是否远离强电磁干扰和热源等环境；

2) 应核查是否有应急处置及检修维护记录。

d) 单元判定：如果 1)或 2)为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2 安全通信网络

8.5.2.1 网络架构

8.5.2.1.1 测评单元(L3-CNS5-01)

该测评单元包括以下要求：

a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段。

b) 测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施包括以下内容：

1) 应核查工业控制系统和企业其他系统之间是否部署单向隔离设备；

2) 应核查是否采用了有效的单向隔离策略实施访问控制；

3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.1.2 测评单元(L3-CNS5-02)

该测评单元包括以下要求:

a) 测评指标:工业控制系统内部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) 测评对象:路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施包括以下内容:

1) 应核查工业控制系统内部是否根据业务特点划分了不同的安全域;

2) 应核查各安全域之间访问控制设备是否配置了有效的访问控制策略。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.5.2.1.3 测评单元(L3-CNS5-03)

该测评单元包括以下要求:

a) 测评指标:涉及实时控制和数据传输的工业控制系统,应使用独立的网络设备组网,在物理层面上实现与其他数据网及外部公共信息网的安全隔离。

b) 测评对象:工业控制系统网络。

c) 测评实施:应核查涉及实时控制和数据传输的工业控制系统是否在物理层面上独立组网。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.5.2.2 通信传输

8.5.2.2.1 测评单元(L3-CNS5-04)

该测评单元包括以下要求:

a) 测评指标:在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

b) 测评对象:加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施:应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.5.3 安全区域边界

8.5.3.1 访问控制

8.5.3.1.1 测评单元(L3-ABS5-01)

该测评单元包括以下要求:

a) 测评指标:应在工业控制系统与企业其他系统之间部署访问控制设备,配置访问控制策略,禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

b) 测评对象:网闸、防火墙、路由器和交换机等提供访问控制功能的设备。

c) 测评实施包括以下内容:

1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备,是否配

置访问控制策略；

2） 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.3.1.2 测评单元（L3-ABS5-02）

该测评单元包括以下要求：

a） 测评指标：应在工业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。

b） 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备，监控预警设备。

c） 测评实施包括以下内容：

1） 应核查设备是否可以在策略失效的时候进行告警；

2） 应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.3.2 拨号使用控制

8.5.3.2.1 测评单元（L3-ABS5-03）

该测评单元包括以下要求：

a） 测评指标：工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施。

b） 测评对象：拨号服务类设备。

c） 测评实施：应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.3.2.2 测评单元（L3-ABS5-04）

该测评单元包括以下要求：

a） 测评指标：拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施。

b） 测评对象：拨号服务类设备。

c） 测评实施：应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.3.3 无线使用控制

8.5.3.3.1 测评单元（L3-ABS5-05）

该测评单元包括以下要求：

a） 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别。

b） 测评对象：无线通信网络及设备。