c) 测评实施包括以下内容：

1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；

2) 应核查用户身份标识是否具有唯一性。

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。

8.5.3.3.2 测评单元(L3-ABS5-06)

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)进行授权以及执行使用进行限制。

b) 测评对象：无线通信网络及设备。

c) 测评实施：应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理，核查未授权的使用是否可以被发现及告警。

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。

8.5.3.3.3 测评单元(L3-ABS5-07)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：无线通信网络及设备。

c) 测评实施：应核查无线通信传输中是否采用加密措施保证传输报文的机密性。

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。

8.5.3.3.4 测评单元(L3-ABS5-08)

该测评单元包括以下要求：

a) 测评指标：对采用无线通信技术进行控制的工业控制系统，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的行为。

b) 测评对象：无线通信网络及设备和监测设备。

c) 测评实施：应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。

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。

8.5.4 安全计算环境

8.5.4.1 控制设备安全

8.5.4.1.1 测评单元(L3-CES5-01)

该测评单元包括以下要求：

a) 测评指标：控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，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。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等功能，如控制设备具备上述功能，则按照通用要求测评；

2) 如控制设备不具备上述功能，则核查是否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。

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。

8.5.4.1.2 测评单元(L3-CES5-02)

该测评单元包括以下要求：

a) 测评指标：应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

1) 应核查是否有测试报告或测试评估记录；

2) 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。

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。

8.5.4.1.3 测评单元(L3-CES5-03)

该测评单元包括以下要求：

a) 测评指标：应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

1) 应核查控制设备是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等；

2) 应核查保留的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等是否通过相关的措施实施严格的监控管理。

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。

8.5.4.1.4 测评单元(L3-CES5-04)

该测评单元包括以下要求：

a) 测评指标：应使用专用设备和专用软件对控制设备进行更新。

b) 测评对象：控制设备。

c) 测评实施：应核查是否使用专用设备和专用软件对控制设备进行更新。

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。

8.5.4.1.5 测评单元(L3-CES5-05)

该测评单元包括以下要求：

a) 测评指标：应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码

程序。

b) 测评对象:控制设备。

c) 测评实施:应核查由相关部门出具或认可的控制设备的检测报告,明确控制设备固件中是否不存在恶意代码程序。

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。

8.5.5 安全建设管理

8.5.5.1 产品采购和使用

8.5.5.1.1 测评单元(L3-CMS5-01)

该测评单元包括以下要求:

a) 测评指标:工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

b) 测评对象:安全管理员和检测报告类文档。

c) 测评实施包括以下内容:

1) 应访谈安全管理员系统使用的工业控制系统重要设备及网络安全专用产品是否通过专业机构的安全性检测;

2) 应核查工业控制系统是否有通过专业机构出具的安全性检测报告。

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。

8.5.5.2 外包软件开发

8.5.5.2.1 测评单元(L3-CMS5-02)

该测评单元包括以下要求:

a) 测评指标:应在外包开发合同中规定针对开发单位、供应商的约束条款,包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

b) 测评对象:外包合同。

c) 测评实施:应核查是否在外包开发合同中规定针对开发单位、供应商的约束条款,包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

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。

9 第四级测评要求

9.1 安全测评通用要求

9.1.1 安全物理环境

9.1.1.1 物理位置选择

9.1.1.1.1 测评单元(L4-PES1-01)

该测评单元包括以下要求:

a) 测评指标:机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 测评对象:记录类文档和机房。

c) 测评实施包括以下内容：

1) 应核查所在建筑物是否具有建筑物抗震设防审批文档；

2) 应核查是否不存在雨水渗漏；

3) 应核查门窗是否不存在因风导致的尘土严重；

4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。

d) 单元判定：如果 1)～4)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。

9.1.1.1.2 测评单元(L4-PES1-02)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：机房。

c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。

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。

9.1.1.2 物理访问控制

9.1.1.2.1 测评单元(L4-PES1-03)

该测评单元包括以下要求：

a) 测评指标：机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

b) 测评对象：机房电子门禁系统。

c) 测评实施包括以下内容：

1) 应核查出入口是否配置电子门禁系统；

2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。

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。

9.1.1.2.2 测评单元(L4-PES1-04)

该测评单元包括以下要求：

a) 测评指标：重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

b) 测评对象：机房电子门禁系统。

c) 测评实施包括以下内容：

1) 应核查重要区域出入口是否配置第二道电子门禁系统；

2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。

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。

9.1.1.3 防盗窃和防破坏

9.1.1.3.1 测评单元(L4-PES1-05)

该测评单元包括以下要求：

a) 测评指标：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识。

b) 测评对象:机房设备或主要部件。

c) 测评实施包括以下内容:

1) 应核查机房内设备或主要部件是否固定;

2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标识。

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。

9.1.1.3.2 测评单元(L4-PES1-06)

该测评单元包括以下要求:

a) 测评指标:应将通信线缆铺设在隐蔽安全处。

b) 测评对象:机房通信线缆。

c) 测评实施:应核查机房内通信线缆是否铺设在隐蔽安全处,如桥架中等。

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。

9.1.1.3.3 测评单元(L4-PES1-07)

该测评单元包括以下要求:

a) 测评指标:应设置机房防盗报警系统或设置有专人值守的视频监控系统。

b) 测评对象:机房防盗报警系统或视频监控系统。

c) 测评实施包括以下内容:

1) 应核查机房内是否配置防盗报警系统或有专人值守的视频监控系统;

2) 应核查防盗报警系统或视频监控系统是否启用。

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。

9.1.1.4 防雷击

9.1.1.4.1 测评单元(L4-PES1-08)

该测评单元包括以下要求:

a) 测评指标:应将各类机柜、设施和设备等通过接地系统安全接地。

b) 测评对象:机房。

c) 测评实施:应核查机房内机柜、设施和设备等是否进行接地处理。

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。

9.1.1.4.2 测评单元(L4-PES1-09)

该测评单元包括以下要求:

a) 测评指标:应采取措施防止感应雷,例如设置防雷保安器或过压保护装置等。

b) 测评对象:机房防雷设施。

c) 测评实施包括以下内容:

1) 应核查机房内是否设置防感应雷措施;

2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。

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。

9.1.1.5 防火

9.1.1.5.1 测评单元(L4-PES1-10)

该测评单元包括以下要求：

a) 测评指标：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

b) 测评对象：机房防火设施。

c) 测评实施包括以下内容：

1) 应核查机房内是否设置火灾自动消防系统；

2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。

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。

9.1.1.5.2 测评单元(L4-PES1-11)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：机房验收类文档。

c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级。

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。

9.1.1.5.3 测评单元(L4-PES1-12)

该测评单元包括以下要求：

a) 测评指标：应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

b) 测评对象：机房管理员和机房。

c) 测评实施包括以下内容：

1) 应访谈机房管理员是否进行了区域划分；

2) 应核查各区域间是否采取了防火措施进行隔离。

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。

9.1.1.6 防水和防潮

9.1.1.6.1 测评单元(L4-PES1-13)

该测评单元包括以下要求：

a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b) 测评对象：机房。

c) 测评实施：应核查机房的窗户、屋顶和墙壁是否采取了防雨水渗透的措施。

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。

9.1.1.6.2 测评单元(L4-PES1-14)

该测评单元包括以下要求：

a) 测评指标: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。
b) 测评对象:机房。
c) 测评实施包括以下内容:
   1) 应核查机房内是否采取了防止水蒸气结露的措施;
   2) 应核查机房内是否采取了排泄地下积水,防止地下积水渗透的措施。
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。

9.1.1.6.3 测评单元(L4-PES1-15)

该测评单元包括以下要求:
a) 测评指标:应安装对水敏感的检测仪表或元件,对机房进行防水检测和报警。
b) 测评对象:机房漏水检测设施。
c) 测评实施包括以下内容:
   1) 应核查机房内是否安装了对水敏感的检测装置;
   2) 应核查防水检测和报警装置是否启用。
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。

9.1.1.7 防静电

9.1.1.7.1 测评单元(L4-PES1-16)

该测评单元包括以下要求:
a) 测评指标:应采用防静电地板或地面并采用必要的接地防静电措施。
b) 测评对象:机房。
c) 测评实施包括以下内容:
   1) 应核查机房内是否安装了防静电地板或地面;
   2) 应核查机房内是否采用了接地防静电措施。
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。

9.1.1.7.2 测评单元(L4-PES1-17)

该测评单元包括以下要求:
a) 测评指标:应采取措施防止静电的产生,例如采用静电消除器、佩戴防静电手环等。
b) 测评对象:机房。
c) 测评实施:应核查机房内是否配备了防静电设备。
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。

9.1.1.8 温湿度控制

9.1.1.8.1 测评单元(L4-PES1-18)

该测评单元包括以下要求:
a) 测评指标:应设置温湿度自动调节设施,使机房温湿度的变化在设备运行所允许的范围之内。
b) 测评对象:机房温湿度调节设施。

c) 测评实施包括以下内容：

1) 应核查机房是否配备了专用空调；

2) 应核查机房内温湿度是否在设备运行所允许的范围之内。

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。

9.1.1.9 电力供应

9.1.1.9.1 测评单元(L4-PES1-19)

该测评单元包括以下要求：

a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备。

b) 测评对象：机房供电设施。

c) 测评实施：应核查机房供电线路上是否配置了稳压器和过电压防护设备。

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。

9.1.1.9.2 测评单元(L4-PES1-20)

该测评单元包括以下要求：

a) 测评指标：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

b) 测评对象：机房供电设施。

c) 测评实施包括以下内容：

1) 应核查是否配备 UPS 等后备电源系统；

2) 应核查 UPS 等后备电源系统是否满足设备在断电情况下的正常运行要求。

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。

9.1.1.9.3 测评单元(L4-PES1-21)

该测评单元包括以下要求：

a) 测评指标：应设置冗余或并行的电力电缆线路为计算机系统供电。

b) 测评对象：机房管理员和机房。

c) 测评实施包括以下内容：

1) 应访谈机房管理员机房供电是否来自两个不同的变电站；

2) 应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。

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。

9.1.1.9.4 测评单元(L4-PES1-22)

该测评单元包括以下要求：

a) 测评指标：应提供应急供电设施。

b) 测评对象：机房应急供电设施。

c) 测评实施包括以下内容：

1) 应核查是否配置了应急供电设施；

2) 应核查应急供电设施是否可用。

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。

9.1.1.10 电磁防护

9.1.1.10.1 测评单元(L4-PES1-23)

该测评单元包括以下要求：

a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰。

b) 测评对象：机房线缆。

c) 测评实施：应核查机房内电源线缆和通信线缆是否隔离铺设。

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。

9.1.1.10.2 测评单元(L4-PES1-24)

该测评单元包括以下要求：

a) 测评指标：应对关键设备或关键区域实施电磁屏蔽。

b) 测评对象：机房关键设备或区域。

c) 测评实施包括以下内容：

1) 应核查机房内是否针对关键区域实施了电磁屏蔽；

2) 应核查机房内是否为关键设备配备了电磁屏蔽装置。

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。

9.1.2 安全通信网络

9.1.2.1 网络架构

9.1.2.1.1 测评单元(L4-CNS1-01)

该测评单元包括以下要求：

a) 测评指标：应保证网络设备的业务处理能力满足业务高峰期需要。

b) 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足需要；

2) 应核查网络设备是否从未出现过因设备性能问题导致的宕机情况；

3) 应测试验证设备是否满足业务高峰期需求。

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。

9.1.2.1.2 测评单元(L4-CNS1-02)

该测评单元包括以下要求：

a) 测评指标：应保证网络各个部分的带宽满足业务高峰期需要。

b) 测评对象：综合网管系统等。

c) 测评实施包括以下内容：

1） 应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要；
2） 应测试验证网络带宽是否满足业务高峰期需求。

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。

9.1.2.1.3 测评单元（L4-CNS1-03）

该测评单元包括以下要求：

a） 测评指标：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
b） 测评对象：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。
c） 测评实施包括以下内容：
1） 应核查是否依据重要性、部门等因素划分不同的网络区域；
2） 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。
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。

9.1.2.1.4 测评单元（L4-CNS1-04）

该测评单元包括以下要求：

a） 测评指标：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。
b） 测评对象：网络管理员和网络拓扑。
c） 测评实施包括以下内容：
1） 应核查网络拓扑图是否与实际网络运行环境一致；
2） 应核查重要网络区域是否未部署在网络边界处；
3） 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL）等。
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。

9.1.2.1.5 测评单元（L4-CNS1-05）

该测评单元包括以下要求：

a） 测评指标：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，保证系统的可用性。
b） 测评对象：网络管理员和网络拓扑。
c） 测评实施：应核查是否有关键网络设备、安全设备和关键计算设备的硬件冗余（主备或双活等）和通信线路冗余。
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。

9.1.2.1.6 测评单元（L4-CNS1-06）

该测评单元包括以下要求：

a） 测评指标：应按照业务服务的重要程度分配带宽，优先保障重要业务。
b） 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备或相关组件。
c） 测评实施：应核查带宽控制设备是否按照业务服务的重要程度配置并启用了带宽策略。
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。

9.1.2.2 通信传输

9.1.2.2.1 测评单元(L4-CNS1-07)

该测评单元包括以下要求:

a) 测评指标:应采用密码技术保证通信过程中数据的完整性。

b) 测评对象:提供密码技术功能的设备或组件。

c) 测评实施包括以下内容:

1) 应核查是否在数据传输过程中使用密码技术来保证其完整性;

2) 应测试验证密码技术设备或组件能否保证通信过程中数据的完整性。

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。

9.1.2.2.2 测评单元(L4-CNS1-08)

该测评单元包括以下要求:

a) 测评指标:应采用密码技术保证通信过程中数据的保密性。

b) 测评对象:提供密码技术功能的设备或组件。

c) 测评实施包括以下内容:

1) 应核查是否在通信过程中采取保密措施,具体采用哪些技术措施;

2) 应测试验证在通信过程中是否对数据进行加密。

d) 单元判定:如果 1)和 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。

9.1.2.2.3 测评单元(L4-CNS1-09)

该测评单元包括以下要求:

a) 测评指标:应在通信前基于密码技术对通信的双方进行验证或认证。

b) 测评对象:提供密码技术功能的设备或组件。

c) 测评实施:应核查是否能在通信双方建立连接之前利用密码技术进行会话初始化验证或认证。

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。

9.1.2.2.4 测评单元(L4-CNS1-10)

该测评单元包括以下要求:

a) 测评指标:应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

b) 测评对象:提供密码技术功能的设备或组件。

c) 测评实施包括以下内容:

1) 应核查是否基于硬件密码模块产生密钥并进行密码运算;

2) 应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。

d) 单元判定:如果 1)和 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。

9.1.2.3 可信验证

9.1.2.3.1 测评单元(L4-CNS1-11)

该测评单元包括以下要求：

a) 测评指标：可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

b) 测评对象：提供可信验证的设备或组件、提供集中审计功能的系统。

c) 测评实施包括以下内容：

1) 应核查是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证；

2) 应核查是否在应用程序的所有执行环节进行动态可信验证；

3) 应测试验证当检测到通信设备的可信性受到破坏后是否进行报警；

4) 应测试验证结果是否以审计记录的形式送至安全管理中心；

5) 应核查是否能够进行动态关联感知。

d) 单元判定：如果1)～5)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。

9.1.3 安全区域边界

9.1.3.1 边界防护

9.1.3.1.1 测评单元(L4-ABS1-01)

该测评单元包括以下要求：

a) 测评指标：应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查在网络边界处是否部署访问控制设备；

2) 应核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略；

3) 应采用其他技术手段(如非法无线网络设备定位、核查设备配置信息等)核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信。

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。

9.1.3.1.2 测评单元(L4-ABS1-02)

该测评单元包括以下要求：

a) 测评指标：应能够对非授权设备私自联到内部网络的行为进行检查或限制。

b) 测评对象：终端管理系统或相关设备。

c) 测评实施包括以下内容：

1) 应核查是否采用技术措施防止非授权设备接入内部网络；

2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。

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。

9.1.3.1.3 测评单元(L4-ABS1-03)

该测评单元包括以下要求：

a) 测评指标：应能够对内部用户非授权联到外部网络的行为进行检查或限制。

b) 测评对象：终端管理系统或相关设备。

c) 测评实施：应核查是否采用技术措施防止内部用户存在非法外联行为。

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。

9.1.3.1.4 测评单元(L4-ABS1-04)

该测评单元包括以下要求：

a) 测评指标：应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

b) 测评对象：网络拓扑和无线网络设备。

c) 测评实施包括以下内容：

1) 应核查无线网络的部署方式，是否单独组网后再连接到有线网络；

2) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。

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。

9.1.3.1.5 测评单元(L4-ABS1-05)

该测评单元包括以下要求：

a) 测评指标：应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断。

b) 测评对象：终端管理系统或相关设备。

c) 测评实施包括以下内容：

1) 应核查是否采用技术措施能够对非授权设备接入内部网络的行为进行有效阻断；

2) 应核查是否采用技术措施能够对内部用户非授权联到外部网络的行为进行有效阻断；

3) 应测试验证是否能够对非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为进行有效阻断。

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。

9.1.3.1.6 测评单元(L4-ABS1-06)

该测评单元包括以下要求：

a) 测评指标：应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。

b) 测评对象：终端管理系统或相关设备。

c) 测评实施包括以下内容：

1) 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证；

2) 应测试验证是否能够对连接到内部网络的设备进行可信验证。

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。

9.1.3.2 访问控制

9.1.3.2.1 测评单元(L4-ABS1-07)

该测评单元包括以下要求：

a) 测评指标：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略；

2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。

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。

9.1.3.2.2 测评单元(L4-ABS1-08)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否不存在多余或无效的访问控制策略；

2) 应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理。

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。

9.1.3.2.3 测评单元(L4-ABS1-09)

该测评单元包括以下要求：

a) 测评指标：应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。

c) 测评实施包括以下内容：

1) 应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；

2) 应测试验证访问控制策略中设定的相关配置参数是否有效。

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。

9.1.3.2.4 测评单元(L4-ABS1-10)

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力；
   2) 应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。
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。

9.1.3.2.5 测评单元(L4-ABS1-11)

该测评单元包括以下要求：
a) 测评指标：应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。
b) 测评对象：网闸等提供通信协议转换或通信协议隔离功能的设备或相关组件。
c) 测评实施包括以下内容：
   1) 应核查是否采取通信协议转换或通信协议隔离等方式进行数据交换；
   2) 应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。
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。

9.1.3.3 入侵防范

9.1.3.3.1 测评单元(L4-ABS1-12)

该测评单元包括以下要求：
a) 测评指标：应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
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) 应核查相关系统或组件是否能够检测从外部发起的网络攻击行为；
   2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；
   3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；
   4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。
d) 单元判定：如果 1)～4)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。

9.1.3.3.2 测评单元(L4-ABS1-13)

该测评单元包括以下要求：
a) 测评指标：应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
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) 应核查相关系统或组件是否能够检测到从内部发起的网络攻击行为；
   2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；
   3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；