NERCIS
信息安全共性技术国家工程研究中心

《网络安全等级保护条例》
《网络安全等保2.0》内容概述

中国科学院信息工程研究所
信息安全共性技术国家工程研究中心

NERCIS
信息安全共性技术国家工程研究中心

目录

NERCIS
信息安全共性技术国家工程研究中心

《网络安全等级保护条例》（征求意见稿）

为贯彻落实《中华人民共和国网络安全法》，深入推进实施国家网络安全等级保护制度，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》。法规框架是八章73条，第一章 总则，第二章 支持与保障，第三章 网络的安全保护，第四章 涉密网络的安全保护，第五章 密码管理，第六章 监督管理，第七章 法律责任，第八章 附则。

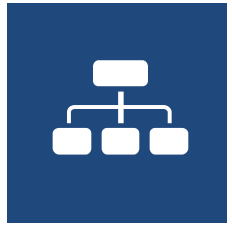
该条例是网络安全法的接续性法规，是网络安全法律体系的重要组成部分，是由国家批准的规范性的法律文件，它具有法的效力。

NERCIS
信息安全共性技术国家工程研究中心

（一）、立法宗旨、适用范围和原则：

【立法宗旨与依据】

依据《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》等法律，制定本条例。



【适用范围】

在中华人民共和国境内建设、运营、维护、使用网络，开展网络安全等级保护工作以及监督管理，适用本条例。个人及家庭自建自用的网络除外。

【确立制度】

国家实行网络安全等级保护制度，对网络实施分等级保护、分等级监管。

【工作原则】

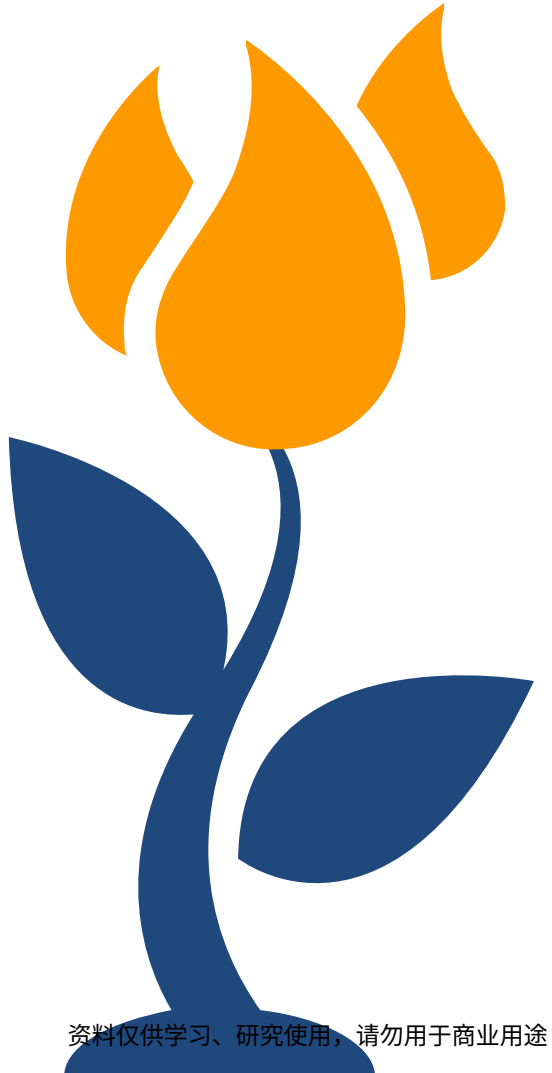
按照**突出重点、主动防御、综合防控**的原则，建立健全网络安全防护体系，重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。

网络运营者在网络建设过程中，应当**同步规划、同步建设、同步运行**网络安全保护、保密和密码保护措施。

NERCIS
信息安全共性技术国家工程研究中心

（二）、职责分工

中央网信机构	统一领导网络安全等级保护工作。
国家网信部门	负责网络安全等级保护工作的统筹协调。
国家公安部门	主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。
国家保密行政管理部门	主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理。
国家密码管理部门	负责网络安全等级保护工作中有关密码管理工作的监督管理。
国务院其他有关部门	依照有关法律法规的规定，在各自职责范围内开展网络安全等级保护相关工作。
县级以上地方人民政府	依照本条例和有关法律法规规定，开展网络安全等级保护工作。



NERCIS
信息安全共性技术国家工程研究中心

（二）、监督管理-公安机关监督管理职责

一、【安全检查】

县级以上公安机关对网络运营者开展网络安全工作情况进行监督检查。

二、【检查处置】

公安机关在监督检查中发现网络安全风险隐患的，应当责令网络运营者采取措施立即消除；不能立即消除的，应当责令其限期整改。

三、【重大隐患处置】

公安机关发现重要行业或本地区存在严重威胁国家安全、公共安全和社会公共利益的重大风险隐患的，应报告同级政府、网信部门和上级公安机关。

四、【对测评机构和安全建设机构的监管】

国家对网络安全等级测评机构和安全建设机构实行推荐目录管理，非涉密网络安全等级测评机构和安全建设机构具体管理办法，由国务院公安部门制定。保密科技测评机构管理办法由国家保密行政管理部门制定。

五、【关键人员管理】

第三级以上网络运营者的关键岗位人员以及为第三级以上网络提供安全服务的人员，不得擅自参加境外组织的网络攻防活动。

六、【事件调查】

公安机关应当根据有关规定处置网络安全事件，开展事件调查，认定事件责任，依法查处危害网络安全的违法犯罪活动。紧急情况下断网。

县级以上公安机关对网络运营者依照国家法律法规规定和相关标准规范要求，落实网络安全等级保护制度，开展网络安全防范、网络安全事件应急处置、重大活动网络安全保护等工作，实行监督管理；对三级以上网络运营者进行重点监督管理。

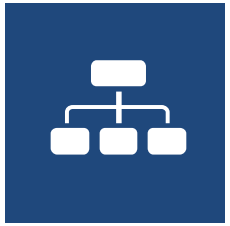
三：监督管理-其他机构的监督管理职责

【保密监督管理】

保密行政管理部门负责对涉密网络的安全保护工作进行监督管理，负责对非涉密网络的失泄密行为的监管。

【行业监督管理】

行业主管部门应当组织制定本行业并监督管理本领域网络安全等级保护工作规划和标准规范，掌握网络基本情况、定级备案情况和安全保护状况；监督管理本行业、本领域网络运营者开展网络定级备案、等级测评、安全建设整改、安全自查等工作。



【密码监督管理】

密码管理部门负责对网络安全等级保护工作中的密码管理进行监督管理，监督检查网络运营者对网络的密码配备、使用、管理和密码评估情况。其中重要涉密信息系统每两年至少开展一次监督检查。

【监督管理责任】

.网络安全等级保护监督管理部门及其工作人员应当对在履行职责中知悉的国家秘密、个人信息和重要数据严格保密，不得泄露、出售或者非法向他人提供。

NERCIS
信息安全共性技术国家工程研究中心

四、支持与保障

【总体保障】

国家建立健全网络安全等级保护制度的组织领导体系、技术支持体系和保障体系。

各级人民政府和行业主管部门应当将网络安全等级保护制度实施纳入信息化工作总体规划，统筹推进。

【标准制定】

国家建立完善网络安全等级保护标准体系。国务院标准化行政主管部门和国务院公安部门、国家保密行政管理部门、国家密码管理部门根据各自职责，组织制定网络安全等级保护的国家标准、行业标准。

【投入和保障】

各级人民政府鼓励扶持网络安全等级保护重点工程和项目，支持网络安全等级保护技术的研究开发和应用，推广安全可信的网络产品和服务。

【技术支持】

国家建设网络安全等级保护专家队伍和等级测评、安全建设、应急处置等技术支持体系，为网络安全等级保护制度提供支撑。

【绩效考核】

行业主管部门、各级人民政府应当将网络安全等级保护工作纳入绩效考核评价、社会治安综合治理考核等。

NERCIS
信息安全共性技术国家工程研究中心

五、网络等级

根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。

第一级 一般网络

一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络。

第二级 一般网络

一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络。

第三级 重要网络

一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。

第四级 特别重要网络

一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络。

第五级 极其重要网络

一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

NERCIS
信息安全共性技术国家工程研究中心

六、定级备案

【网络定级】

- 网络运营者应当在规划设计阶段确定网络的安全保护等级。

【定级评审】

- 对拟定为第二级以上的网络，其运营者应当组织专家评审；有行业主管部门的，应当在评审后报请主管部门核准。
- 跨省或者全国统一联网运行的网络由行业主管部门统一拟定安全保护等级，统一组织定级评审。

【定级备案】

- 第二级以上网络运营者应当在网络的安全保护等级确定后10个工作日内，到县级以上公安机关备案。

【备案审核】

- 公安机关应当对网络运营者提交的备案材料进行审核。对定级准确、备案材料符合要求的，应在10个工作日内出具网络安全等级保护备案证明。

NERCIS
信息安全共性技术国家工程研究中心

七、【特殊安全保护义务】第三级以上网络的运营者除履行本条例第二十条规定的网络安全保护义务外，还应当履行下列安全保护义务：

（一）确定网络安全管理机构，明确网络安全等级保护的工作职责，

（二）制定并落实网络安全总体规划和整体安全防护策略，制定安全建设方案，并经专业技术人员评审通过；

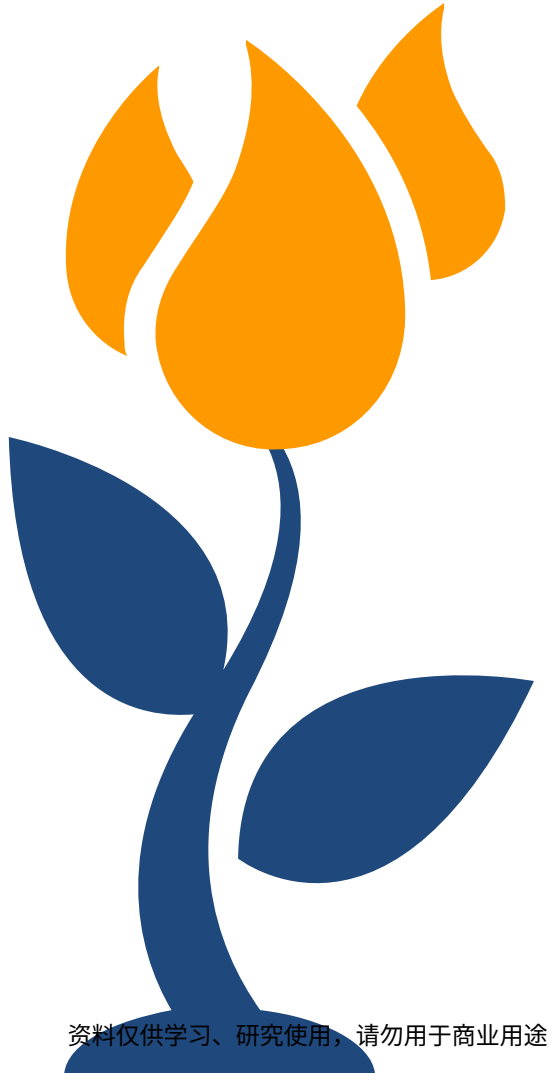
（三）对网络安全管理负责人和关键岗位的人员进行安全背景审查，落实持证上岗制度；

（四）对为其提供网络设计、建设、运维和技术服务的机构和人员进行安全管理；

（五）落实网络安全态势感知监测预警措施，

（六）落实重要网络设备、通信链路、系统的冗余、备份和恢复措施；

（七）建立网络安全等级测评制度，定期开展等级测评，并将测评情况及安全整改措施、整改结果向公安机关和有关部门报告；



NERCIS
信息安全共性技术国家工程研究中心

四、涉密网络的安全保护（1）

【分级保护】	【网络定级】	【方案审查论证】	【建设管理】	【信息设备、安全保密产品管理】
涉密网络按照存储、处理、传输国家秘密的最高密级分为绝密级、机密级和秘密级。	涉密网络运营者应当依法确定涉密网络的密级，通过本单位保密委员会（领导小组）的审定，并向同级保密行政管理部门备案。	涉密网络运营者规划建设涉密网络，应当依据国家保密规定和标准要求，制定分级保护方案，	涉密网络运营者委托其他单位承担涉密网络建设的，应当选择具有相应涉密信息系统集成资质的单位，并与建设单位签订保密协议，明确保密责任，采取保密措施。	涉密网络中使用的信息设备，应当从国家有关主管部门发布的涉密专用信息设备名录中选择；未纳入名录的，应选择政府采购目录中的产品。

NERCIS
信息安全共性技术国家工程研究中心

四、涉密网络的安全保护（2）

【测评审查和风险评估】	【涉密网络使用管理总体要求】	【涉密网络预警通报要求】	【涉密网络重大变化的处置】	【涉密网络废止的处理】
涉密网络应当由国家保密行政管理部门设立或者授权的保密测评机构进行检测评估，并经设区的市级以上保密行政管理部门审查合格，方可投入使用。	涉密网络运营者应当依法确定涉密网络的密级，通过本单位保密委员会（领导小组）的审定，并向同级保密行政管理部门备案。	涉密网络运营者应建立健全本单位涉密网络安全保密监测预警和信息通报制度，发现安全风险隐患的，应及时采取应急处置措施，并向保密行政管理部门报告。	涉密网络运营者应当按照国家保密规定及时向保密行政管理部门报告并采取相应措施。	涉密网络不再使用的，涉密网络运营者应当及时向保密行政管理部门报告，并按照国家保密规定和标准对涉密信息设备、产品、涉密载体等进行处理。

NERCIS
信息安全共性技术国家工程研究中心

目录

NERCIS
信息安全共性技术国家工程研究中心

一、网络安全等级保护2.0的概念

信息安全等级保护1.0

以GB17859-1999《计算机信息系统安全保护等级划分则 》为根标准，以GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求 》为基础标准；推动重要信息系统和基础网络的定级、备案、测评、整改、监督检查等工作。将《基本要求》的2008版本及其配套规范标准称为等保1.0。

网络安全等级保护2.0

2014年开始制定2.0标准，修订了通用安全要求，增加了云计算、大数据、移动互联、工控、物联网等安全扩展要求，内容包括 网络安全等级保护基本要求 、安全通用要求和安全扩展要求，标志着等级保护2.0时代的到来。

NERCIS
信息安全共性技术国家工程研究中心

一、网络安全等级保护2.0的概念

网络安全等级保护2.0的三个标准：

- 信息安全技术
网络安全等级保护基本要求 GB/T22239-XXXX

- 信息安全技术
网络安全等级保护安全设计技术要求GB/T25070-XXXX

- 信息安全技术
网络安全等级保护测评要求GB/T28448-XXXX

NERCIS
信息安全共性技术国家工程研究中心

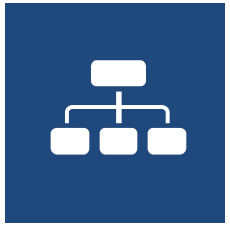
二、网络安全等级保护2.0的基本特点

【法律地位得到确认】

《网络安全法》第21条“国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

【内容进一步完善】

除定级、备案、建设整改、测评和监督检查外，增加了风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等。



【保护对象得到扩展】

主要包括基础信息网络、信息系统（例如工业控制系统、云计 算平台、物联网、使用移动互联技术的信息系统以及其他信息系统）和大数据等。

【制度体系基本形成责任】

.包括：法律政策体系、法规标准体系、技术支撑体系、支撑保障体系、教育培训体系、人才培养体系等。

三、网络安全等级保护2.0的核心内容

将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等重点措施全部纳入等级保护制度并实施。

将网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网、工控系统 、公众服务平台等全部纳入等级保护监管。

将互联网企业纳入等级保护管理，保护互联网企业健康发展。

四、等级保护2.0的重点任务

1、科学确定等级 ：

根据《网络安全等级保护定级指南》（GA/T1389-2017)初步确定安全保护等级。不是自主定级。专家评审，主管部门审核。

2、向公安机关备案。

网络运营者将定级材料向公安机关备案，公安机关审核，对符合要求的发放备案证明。

3、开展等级测评。

网络运营者选择符合国家规定条件的测评机构，对三级以上系统每年开展等级测评

4、安全建设整改。

网络运营者根据系统安全保护等级，按照国家标准开展安全建设整改。

5、监督检查。

公安机关每年开展执法检查。

五、等级保护2.0的扩展与调整

（一）扩充新技术新应用的安全要求

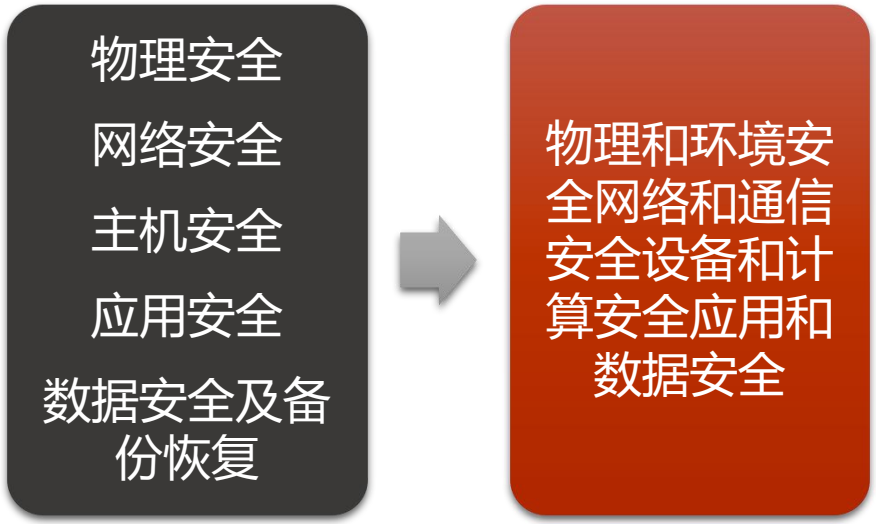
- 第三级安全要求
- 云计算安全扩展要求
- 移动互联安全扩展要求
- 物联网安全扩展要求
- 工业控制系统扩展安全要求

（二）取消安全标注

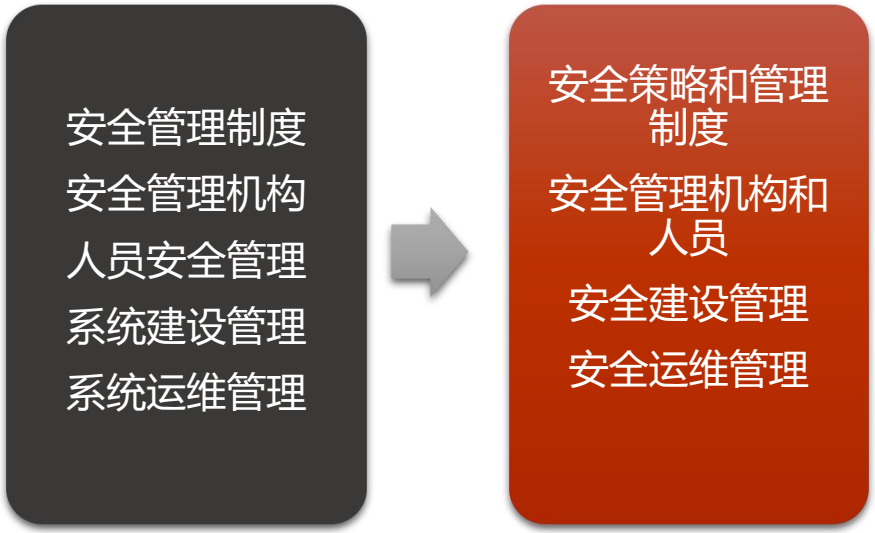
- 取消对控制点的“S”、“A”、“G”标注的使用
- 调整为原来的附录A：“安全要求的选择和使用”，
- 说明与定级指南的关系，增加安全控制措施选择时，控制点的使用和标注及使用说明。

五、等级保护2.0-扩展与调整

（二）调整技术控制措施分结构



（三）调整管理控制措施分类



NERCIS
信息安全共性技术国家工程研究中心

五、等级保护2.0-关键信息基础设施安全要求

(一)	关键信息基础设施的范围必须在定级备案的第三级（含）以上的保护对象中确定。
(二)	关键信息基础设施必须按照等级保护制度要求，开展定级备案、等级测评、安全建设整改、安全检查等强制性、规定性工作。
(三)	公安机关、 保密部门、密码部门在关键信息基础设施保护中要落实保卫、保护、监管责任，网络运营者和行业主管部门要落实主体责任。
(四)	公安机关在情报侦察、追踪溯源、快速处置、打击犯罪、等级保护、通报预警、互联网管理等方面发挥主力军作用。
(五)	等级保护制度是普适性的制度，是关键信息基础设施保护的基础，关键信息基础设施是等级保护制度的保护重点，两者同样重要，不可分割。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-保护对象

基础信息网络

为信息流通、信息系统运行等起基础支撑作用的信息网络，包括电信网、广播电视传输网、互联网、 业务专网等网络设备设施

信息系统

由计算机和类计算机的软硬件及其相关的和配套的设备、设施构成的，按照一定的应用目标和规则进行信息处理或过程控制的资源集合。资源可以是物理设备，也可以是虚拟设备。

国家关键信息基础设施

公共通信和信息服务、能源、金融、交通、水利、公共服务和电子政务等重要行业和领域的基础信 息网络、重要信息系统和数据资源，以及其他一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家 安全、国计民生和公共利益的等级保护对象。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-等级划分

1

第一级

等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；

2

第二级

等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；

3

第三级

等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；

4

第四级

等级保护对象受到破坏后，会对社会秩序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；

5

第五级

等级保护对象受到破坏后，会对国家安全造成特别严重损害

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-保护能力要求

应能够防护系统免受来自**个人的、拥有很少资源**的威胁源发起的恶意攻击、一般的自然灾难，及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第一级安全保护能力

第二级安全保护能力

应能够防护系统免受来自**外部小型组织的**、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害 程度的威胁，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

应能够在统一安全策略下防护系统免受来自**外部有组织的团体**,拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第三级安全保护能力

第四级安全保护能力

应能够在统一安全策略下防护系统免受**来自国家级的、敌对组织的、**拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

六、等级保护2.0的通用要求-恢复能力要求

第一级：

系统具有基本的数据备份功能，在遭到破坏后能够不限时的恢复部分系统功能。

第二级：

系统具有一定的数据备份功能，在遭到破坏后能够在一段时间内恢复部分功能。

第三级：

系统具有较高的数据备份和系统备份功能，在遭到破坏后能够较快的恢复绝大部分功能。

第四级：

系统具有极高的数据备份和系统备份功能，在遭到破坏后能够迅速恢复所有系统功能。

NERCIS
信息安全共性技术国家工程研究中心

七、等级保护2.0的系统定级-定级流程要求

确定定级对象

初步定级

专家评审

二级以上定级，使用单位应组织专家对初步定级结果的合理性进行评审， 出具专家评审意见。

主管部门审核

使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

公安机关备案审查

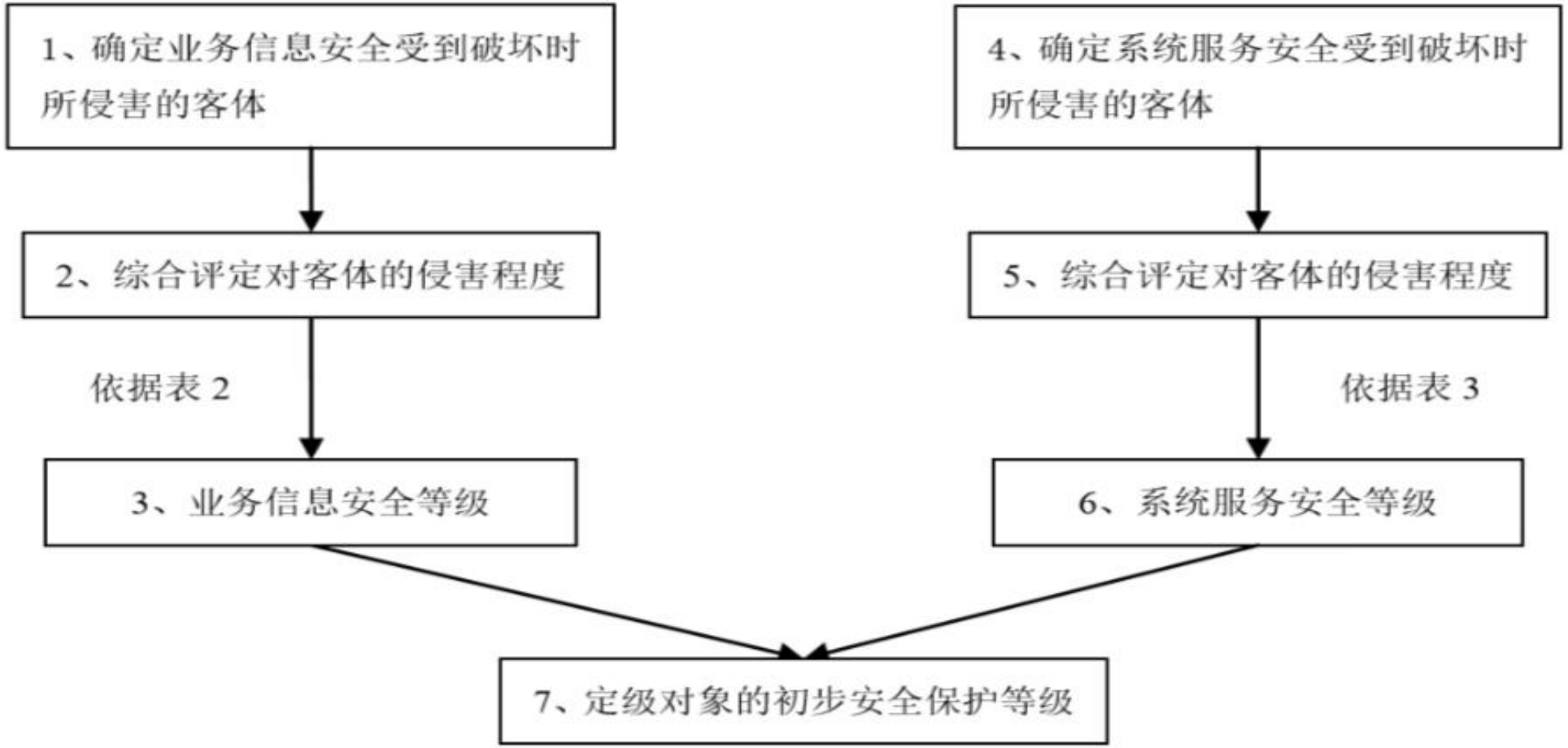
使用单位应将初步定级结果10日内提交公安机关进行备案审查，审查不通过，其使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

等级变更

当等级保护对象所处理的信息、业务状态和系统服务范围发生变化，应根据本标准要求重新确定定级对象和安全保护等级。

NERCIS
信息安全共性技术国家工程研究中心

七、等级保护2.0的系统定级-定级方法流程



六、等级保护2.0的通用要求-定级对象的确定

定级对象	定级要素
基础信息网络	对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。 跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。
信息系统	工业控制系统 工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定原则见5. 2. 5。现场设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。
	云计算平台 在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。
	物联网 物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。
	采用移动互联技术的信息系统 采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线 网络以及相关应用系统等。
大数据	应将具有统一安全责任单位的大数据作为一个整体对象定级，或将其与责任主体相同的相关支撑平台统一定级。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-定级对象的特征

1

a）具有确定的主要安全责任单位。

作为定级对象的信息系统应能够明确其主要安全责任单位；

2

b）承载相对独立的业务应用。

作为定级对象的信息系统应承载相对独立的业务应用，完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；

3

c) 具有信息系统的基本要素。

作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-对客体侵害程度的定义

1

一般损害：

工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律 问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害；

2

严重损害：

工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法 律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害；

3

特别严重损害：

工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行， 出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成 非常严重损害。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0的通用要求-对保护对象的定级要素

受侵害的客体	侵害的事项
公民、法人和其他组织的合法权益	影响社会成员使用公共设施； 影响社会成员获取公开信息资源； 影响社会成员接受公共服务等方面； 其他影响公共利益的事项。 侵害公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所 享有的一定的社会权利和利益等受到损害。
社会秩序、公共利益	影响国家机关社会管理和公共服务的工作秩序； 影响各种类型的经济活动秩序；影响各行业的科研、生产秩序； 影响公众在法律约束和道德规范下的正常生活秩序等； 其他影响社会秩序的事项。
国家安全	影响国家政权稳固和国防实力； 影响国家统一、民族团结和社会安定； 影响国家对外活动中的政治、经济利益； 影响国家重要的安全保卫工作； 影响国家经济竞争力和科技实力； 其他影响国家安全的事项。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0系统定级-对定级要素和保护等级的关系

受侵害的客体	侵害程度	侵害程度	侵害程度
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0系统定级-对业务信息矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表3系统服务安全保护等级矩阵表，即可得到系统服务安全保护等级。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0系统定级-系统服务矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级对象的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。

NERCIS
信息安全共性技术国家工程研究中心

六、等级保护2.0系统定级-确定安全保护等级流程

a）确定受到破坏时所侵害的客体。

1）确定业务信息受到破坏时所侵害的客体； 2）确定系统服务受到侵害时所侵害的客体。

b）确定对客体的侵害程度 。

1）根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度； 2）根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度。

c）确定安全保护等级。

1）确定业务信息安全保护等级；
2）确定系统服务安全保护等级；
3）将业务信息安全保护等级和系统服务安全保护等级的较高者初步确定为定级对象的安全 保护等级

六、等级保护2.0系统定级-确定安全保护等级原则

对于大数据等定级对象，应综合考虑数据规模、数据价值等因素，根据其在国家安全、经济建设、 社会生活中的重要程度，以及数据资源遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定其安全保护等级。原则上大数据安全保护等级为第三级以上。

对于基础信息网络、云计算平台等定级对象，应根据其承载或将要承载的等级保护对象的重要程度 确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。

国家关键信息基础设施的安全保护等级应不低于第三级。

六、等级保护2.0系统定级-确定安全保护等级的建议

第一级信息系统：

乡镇所属信息系统、县级单位中一般的信息系统、小型私营、个体企业、中小学的信息系统。

第二级信息系统

县级单位中的重要信息系统，地市级以上国家机关、企事业单位内部一般的信息系统。非涉及工作秘密、商业秘密、敏感信息的办公和管理系统

第三级信息系统：

地市级以上国家机关、重要企事业单位内部信息系统。涉及工作和商业秘密、敏感信息的办公管理系统，跨省、市联网运行的生产、调度、管理等重要系统，重要系统在省、市的分支，中央各部委、省（区、市）门户网站。

第四级信息系统：

国家重要领域、重要部门中的特别重要系统以及核心系统。例如全国铁路、民航、电力等部门的调度系统，银行、证券、保险、税务、海关等几十个重要行业、部门中的涉及国计民生的核心系统。

第五级信息系统：

国家重要领域、重要部门中的极端重要系统。

NERCIS
信息安全共性技术国家工程研究中心

七、等保2.0-云计算/原则性要求

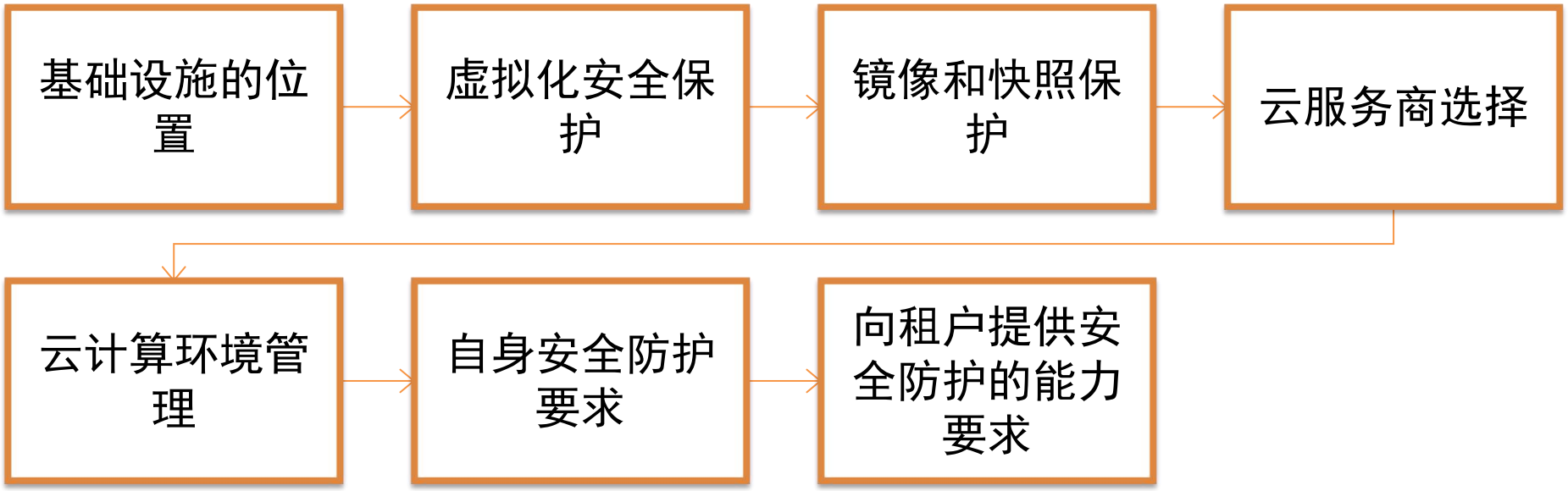
应确保云计算平台不承载高于其安全保护等级的业务应用系统。

应确保云计算基础设施位于中国境内。

云计算平台的运维地点应位于中国境内，如需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。

云计算平台运维过程产生的配置数据、鉴别数据、业务数据、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。

七、等保2.0-云计算/要求要点



七、等保2.0-云计算/扩展要求

a）云计算安全扩展要求-系统定级

- 在云计算环境中，将云计算平台作为基础设施，云客户业务系统作为信息系统，分别作为定级对象定级。
- 对于大型云计算平台，当运管平台共用时，可将云计算基础设施与运管平台系统分开定级。责任分离，分别定级，各自备案。
- 云计算基础设施的安全保护等级不低于其所支撑的业务系统的等级。

b）云计算安全扩展要求-结构

七、等保2.0-云计算/扩展要求

c）云计算安全扩展要求-资源隔离

- 应实现不同云服务客户虚拟网络之间的隔离；
- 应确保云服务客户的虚拟机使用独占的内存空间
- 应保证云计算平台管理流量不于客户业务流量分
- 应保证不同云服务客户的审计数据隔离存放；
- 应保证虚拟机所使用的内存和存储空间回收时得

d）云计算安全扩展要求-访问控制

- 应具有根据云服务客户业务需求自主设置安全策略集的能力，包括定义访问路径、选择安全组件、配置安全策略；
- 实现云平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限； 确保只有在于服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
- 云计算平台应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务。

七、等保2.0-云计算/扩展要求

e）云计算安全扩展要求-数据安全

- 应提供查询云服务客户数据及备份存储位置的方式；
- 保证虚拟机迁移过程中重要数据的完整性和保密性；
- 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- 对虚拟机快照中的敏感信息进行加密保护；
- 支持云服务客户部署密钥管理解决方案，确保云服 务客户自行实现数据的加解密过程 。

f）云计算安全扩展要求-审计与监控

- 能识别、监控虚拟机之间、虚拟机与物理机之间、 虚拟机与宿主机之间的流量；
- 保证云服务商对于服务客户系统和数据的操作可被云服务客户审计；
- 根据云服务方和云客户的职责划分，实现各自控制部分的集中审计；
- 应为安全审计数据的汇集提供接口，可供第三方审计。

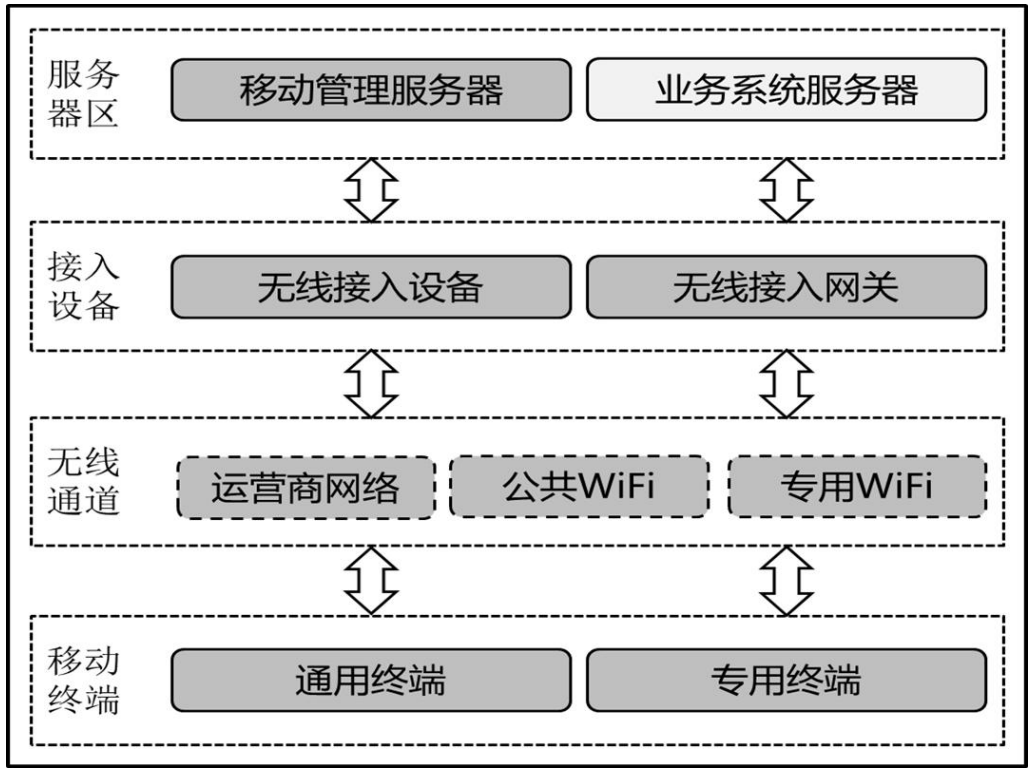
八、等保2.0-移动互联网/扩展要求

移动互联网环境增加要求

- 无线接入点的物理位置
- 移动终端管控
- 移动应用管控
- 移动应用软件采购
- 移动应用软件开发

NERCIS
信息安全共性技术国家工程研究中心

八、等保2.0-移动互联网/扩展要求



适用安全通用要求

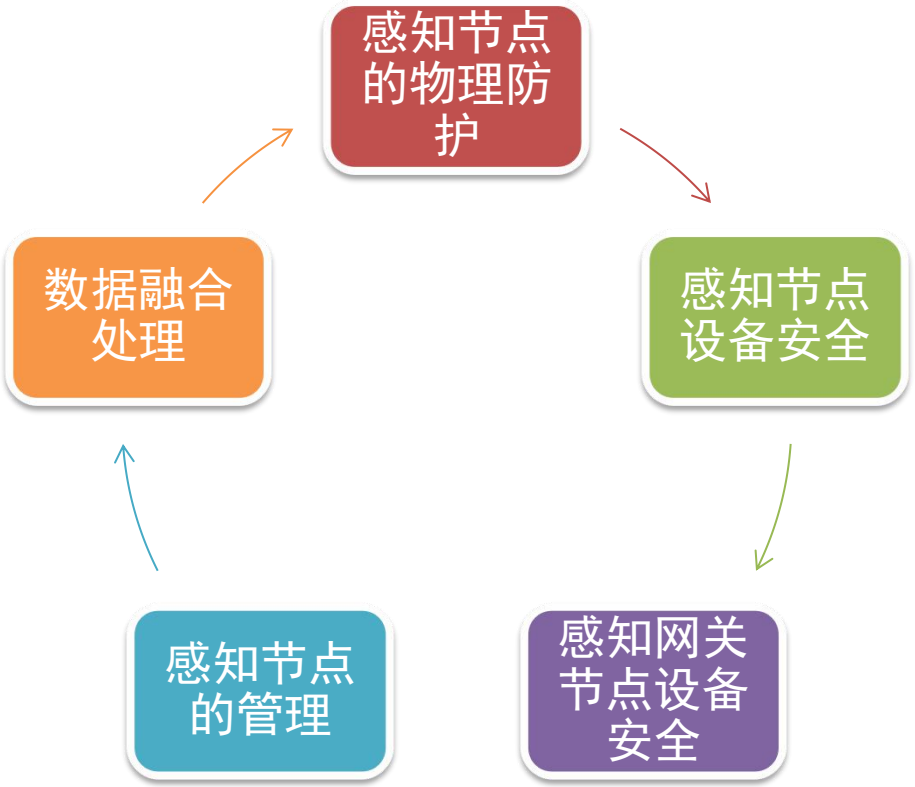
适用安全扩展要求

运营商网络

适用安全扩展要求

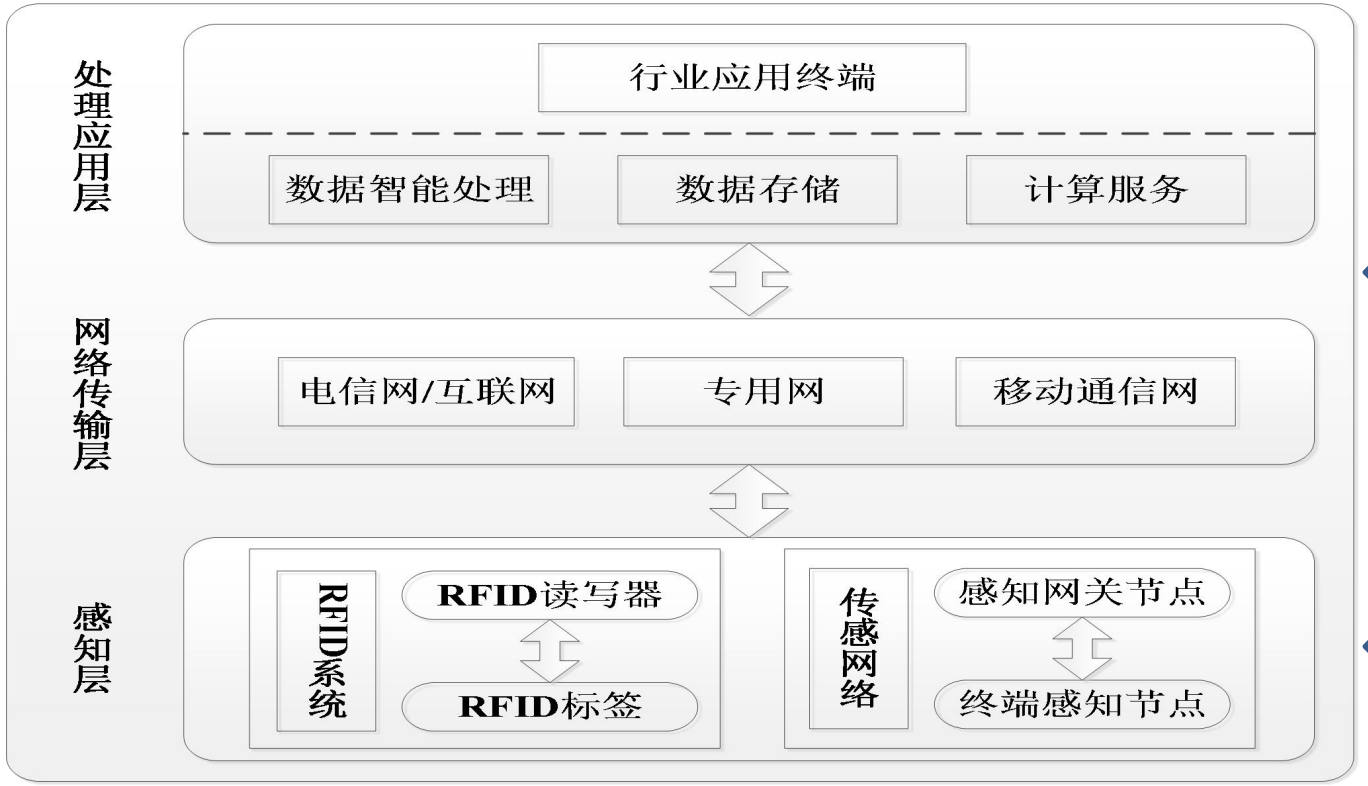
九、等保2.0-物联网/扩展要求

- 物联网 internet of things(IoT)
- 物联网是将感知节点设备通过互联网等网络连接起来构成的一个应用系统，它融合信息系统和物理世界实体，是虚拟世界与现实世界的结合。
- 物联网分为物联网和产业物联网，产业物联网是基于云平台实现安全监控和数据分析的。



NERCIS
信息安全共性技术国家工程研究中心

九、等保2.0-物联网//扩展要求-使用场景



适用安全
通用要求

适用安全
扩展要求

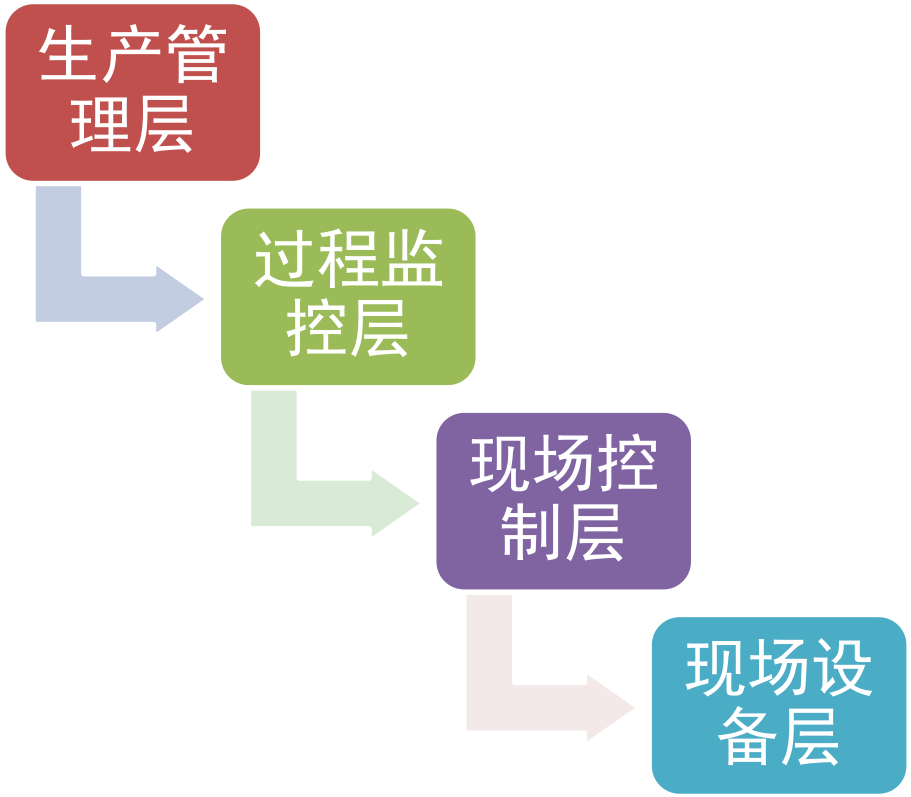
NERCIS
信息安全共性技术国家工程研究中心

十、等保2.0-工业控制系统安全//扩展要求

- 室外控制设备防护
- 工业控制系统网络架构安全
- 拨号使用控制
- 无线使用控制
- 控制设备安全
- 漏洞和风险管理
- 恶意代码防范管理

十、等保2.0-工业控制系统安全//合并于精炼

- 工业控制系统安全扩展要求主要针对现场控制层和现场设备层提出特殊安全要求，其他层次使用安全通用要求条款。
- 对工业控制系统的保护需要根据实际情况使用基本要求，具体安全通用要求和安全扩展要求的使用方法比较复杂。



NERCIS
信息安全共性技术国家工程研究中心

十、等保2.0-工业控制系统安全/基本要求参考表

功能层次	技术要求
企业资源层	安全通用要求（物理和环境安全）
	安全通用要求（网络和通信安全）
	安全通用要求（设备和计算安全）
	安全通用要求（应用和数据安全）
生产管理层	安全通用要求（物理和环境安全）
	安全通用要求（网络和通信安全）+安全扩展要求（网络和通信安全）
	安全通用要求（设备和计算安全）
	安全通用要求（应用和数据安全）
过程监控层	安全通用要求（物理和环境安全）
	安全通用要求（网络和通信安全）+安全扩展要求（网络和通信安全）
	安全通用要求（设备和计算安全）
	安全通用要求（应用和数据安全）
现场控制层	安全通用要求（物理和环境安全）+安全扩展要求（物理和环境安全）
	安全通用要求（网络和通信安全）+安全扩展要求（网络和通信安全）
	安全通用要求（设备和计算安全）+安全扩展要求（设备和计算安全）
	安全通用要求（应用和数据安全）+安全扩展要求（应用和数据安全）
现场设备层	安全通用要求（物理和环境安全）+安全扩展要求（物理和环境安全）
	安全通用要求（网络和通信安全）+安全扩展要求（网络和通信安全）
	安全通用要求（设备和计算安全）+安全扩展要求（设备和计算安全）
	安全通用要求（应用和数据安全）+安全扩展要求（应用和数据安全）