# 国家能源局综合司文件

国能综通安全〔2022〕71号

## 国家能源局综合司关于印发《电力行业网络安全等级保护定级指南》的通知

各省（自治区、直辖市）能源局，有关省（自治区、直辖市）及新疆生产建设兵团发展改革委、工业和信息化主管部门，北京市城市管理委，各派出机构，全国电力安全生产委员会各企业成员单位：

为贯彻落实国家网络安全等级保护相关要求，规范电力行业网络安全等级保护定级工作，落实《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》及《信息安全等级保护管理办法》（公通字〔2007〕43号）等法律法规要求，国家能源局组织制定了《电力行业网络安全等级保护定级指南》。现印发给你们，供参照执行。

（此页无正文）

国家能源局综合司

2022年7月15日

（不公开）

# 电力行业网络安全等级保护定级指南

## 一、引言

为贯彻落实国家网络安全等级保护相关要求，规范电力行业网络安全等级保护定级工作，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》及《信息安全技术 网络安全等级保护定级指南》（GB/T 22240—2020）等法律法规和标准规范，制定本指南。

本指南给出了电力行业网络安全等级保护定级的基本原理、技术方法和部分重要等级保护对象定级建议。网络安全等级保护定级的工作组织和管理流程遵照国家和电力行业网络安全等级保护相关法律法规和规范性文件执行。

电力企业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定级工作，适用本指南。

## 二、依据

《中华人民共和国网络安全法》

《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令第147号）

《信息安全等级保护管理办法》（公通字〔2007〕43号）

《电力监控系统安全防护规定》（中华人民共和国国家发展和

改革委员会令2014年第14号）

《电力监控系统安全防护总体方案等安全防护方案和评估规范》（国能安全〔2015〕36号）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240—2020）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058—2019）

《电力监控系统网络安全防护导则》（GB/T 36572—2018）

## 三、术语和定义

### （一）网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

### （二）等级保护对象

网络安全等级保护工作直接作用的对象。在进行等级保护定级时，将待定级的等级保护对象称为定级对象。

### （三）信息系统

应用、服务、信息技术资产或其他信息处理组件的组合。通常由计算机或者其他信息终端及相关设备组成，按照一定的应用目标和规则进行信息处理或过程控制。典型的信息系统如办公自动化系统、云计算平台/系统、物联网、工业控制系统以及采用移动互联技术的系统等。电力行业信息系统通常从业务维度分为电力监控系统

和管理信息系统。

（四）电力监控系统

用于监视和控制电力生产及供应过程的信息系统。包括电力数据采集与监控系统（SCADA）、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统等。

（五）管理信息系统

用于支撑企业日常经营及办公管理、面向社会大众提供电力等综合服务的信息系统。包括办公自动化系统、财务管控系统、营销业务系统、客户服务系统、内/外部网站、邮件系统等。

（六）通信网络设施

为信息流通、网络运行等起基础支撑作用的网络设备设施。包括电信运营商公网、电力调度数据网络、电力企业自建专用通信网络等。

（七）数据资源

具有或预期具有价值的数据集合。多以电子形式存在。

（八）受侵害的客体

受法律保护的、等级保护对象受到破坏时所侵害的社会关系。简称“客体”。

（九）客观方面

对客体造成侵害的客观外在表现，包括侵害方式和侵害结果等。

## 四、定级原理

### （一）安全保护等级

根据在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、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、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素，电力行业网络安全等级保护对象分为五个安全保护等级：

第一级，受到破坏后，会对公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益。

第二级，受到破坏后，会对公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全。

第三级，受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害。

第四级，受到破坏后，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。

第五级，受到破坏后会对国家安全造成特别严重危害。

### （二）定级要素

等级保护对象的定级要素包括：受侵害的客体、对客体的侵害程度。

1.受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

（1）公民、法人和其他组织的合法权益；

（2）社会秩序、公共利益；

（3）国家安全。

2.对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

（1）造成一般损害；

（2）造成严重损害；

（3）造成特别严重损害。

### （三）定级要素与安全保护等级的关系

定级要素与安全保护等级的关系如表1所示。

表1 定级要素与安全保护等级的关系

| 受侵害的客体 | 对客体的侵害程度 | | |
|---|---|---|---|
| | 一般损害 | 严重损害 | 特别严重损害 |
| 其他公民、法人和组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 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 |

## 五、定级方法

### （一）定级步骤

电力行业网络安全等级保护定级分为图1所示四个步骤：

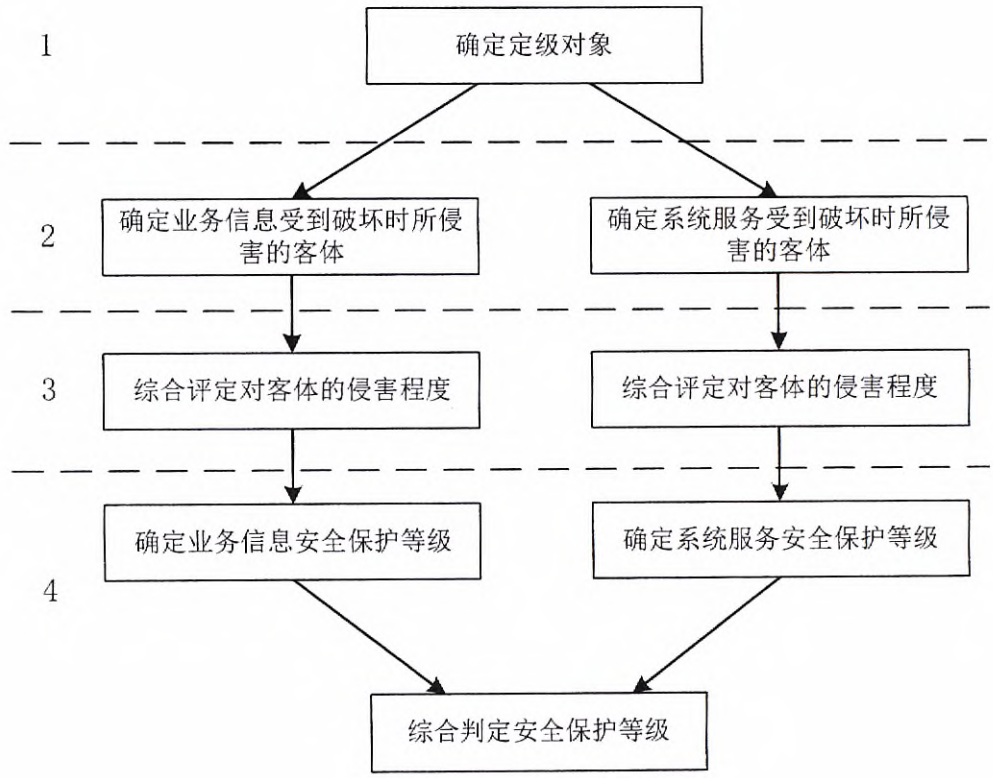


图 1 定级步骤

1.确定定级对象；

2.确定受侵害的客体；

3.确定对客体的侵害程度；

4.综合判定安全保护等级。

具体方法在本章后面各节描述。

按照上述步骤确定定级对象及其安全保护等级后，应按照国家和电力行业网络安全等级保护有关管理要求，组织专家评审、报送主管部门审核和公安机关备案，最终确定其安全保护等级。

（二）确定定级对象

GB/T 22240—2020 将网络安全等级保护对象划分为信息系统、

通信网络设施和数据资源三大类。按照电力行业对信息系统的一般分类，本指南将电力行业网络安全等级保护对象进一步划分为电力监控系统、管理信息系统、通信网络设施、数据资源和其他系统平台五大类。其中，电力监控系统、管理信息系统和其他系统平台统属于“信息系统”类对象。

按照《电力监控系统安全防护规定》，电力监控系统包含作为基础支撑的通信及数据网络，如电力调度数据网络等。本指南参照GB/T 22240—2020，将电力监控系统中的基础支撑通信网络划入“通信网络设施”类进行分析。

针对各类对象确定定级对象需考虑以下因素。

1.信息系统

作为定级对象的所有信息系统均应满足以下（1）描述的三个基本特征。在此基础上，电力监控系统定级对象的确定还应遵循（2）的有关要求。此外，对于采用云计算、物联网、移动互联技术的系统，还应分别遵循以下（3）（4）（5）的相关要求。

（1）定级对象的基本特征

①具有确定的主要安全责任主体。安全责任主体承担信息系统规划建设、运行维护等过程的全部安全责任。安全责任主体可以为电力企业及其各级下属单位。

②承载相对独立的业务应用。定级对象承载业务应用的主要业务流程应相对独立、完整，与其他业务应用之间的应用交互和数据交换应通过比较明确的边界、接口。定级对象可能会与其他业务应

用共享一些设备，尤其是网络传输设备。

③包含相互关联的多个资源。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有形实体。应避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。

（2）电力监控系统

电力监控系统包括现场采集执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集执行、现场控制和过程控制等要素需作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级。

对于大型电力监控系统，可根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象，也可以作为一个整体进行统一定级。例如，变电站监控系统可按照安全管理责任主体作为独立系统定级，也可作为上级调度机构的调度自动化系统子站统一定级；火电厂/水电站 DCS 系统可根据控制对象和生产厂商按机组划分定级对象，也可以按厂站统一定级。如果作为一个整体定级，应在后续定级分析时充分考虑其各组成部分受到破坏后对客体侵害程度的关联影响。

（3）云计算平台/系统

电力企业租用云服务商的云计算平台，应按照前面要求对部署在云计算平台上的系统划分定级对象。云计算平台由云服务商负责定级。

电力企业自建云计算平台时，除应按照前面要求对部署在云计算平台上的系统划分定级对象外，还应将云计算平台作为单独的定级对象定级。对于大型云计算平台，宜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。

云计算平台安全保护等级应不低于部署在云计算平台上的系统的安全保护等级。

（4）电力物联网

电力物联网包括感知、网络传输和处理应用等特征要素，需将以上要素作为一个整体对象定级，各要素不单独定级。

（5）采用移动互联技术的系统

采用移动互联技术的系统主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

2.通信网络设施

对于电力调度数据网和电力企业自建的电力企业数据网等大型通信网络设施，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。当安全责任主体相同时，可作为一个整体对象定级；当安全责任主体不同时，需根据安全责任主体和服务区域划分为若干个定级对象。例如，对于电力调度数据网，可将集团总部管辖的省级及以上网络与二级单位管辖的省级以下网络划分为不同定级对象。

3.数据资源

数据资源可独立定级。当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体对象定级；当安全责任主体不同时，大数据与大数据平台/系统应独立定级，且大数据平台/系统安全保护等级应不低于大数据的安全保护等级。

（三）确定受侵害的客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益。GB/T 22240—2020给出了侵害各类客体的事项描述。

确定受侵害的客体时，首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公共利益，最后判断是否侵害公民、法人和其他组织的合法权益。

（四）确定对客体的侵害程度

1.侵害的客观方面

在客观方面，对客体的侵害外在表现为对定级对象的破坏，其侵害方式表现为对业务信息安全的破坏和对系统服务安全的破坏。其中，业务信息安全是指确保等级保护对象中信息的保密性、完整性和可用性等；系统服务安全是指确保等级保护对象可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种侵害方式。

业务信息安全和系统服务安全受到破坏后，可能产生以下侵害后果：

（1）影响行使工作职能；

（2）导致业务能力下降；

（3）引起法律纠纷；

（4）导致财产损失；

（5）造成社会不良影响；

（6）对其他组织和个人造成损失；

（7）其他影响。

2.综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同侵害后果分别确定其侵害程度。对不同侵害后果确定其侵害程度所采取的方法和所考虑的角度可能不同，例如，系统服务安全被破坏导致业务能力下降的程度，可以从定级对象服务覆盖的区域范围、用户人数或业务量等不同方面确定；业务信息安全被破坏导致的财物损失，可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

参照 GB/T 22240—2020，表 2 给出了电力行业等级保护对象受到破坏后的危害程度的一般描述，表 3 给出了电力行业各类等级保护对象受到破坏后可能侵害的客体与侵害程度。

表 2 电力行业等级保护对象受破坏后的危害程度

| 侵害的客体 | 一般损害 | 严重损害 | 特别严重损害 |
| --- | --- | --- | --- |
| 其他公民、法人和组织的合法权益 | 对电力企业造成一定的经济损失，或对个别公民、法人或其它组织的利益造成较低 | 对电力企业造成严重的经济损失，或对众多公民、法人或其它组织的利益造成严重的损害。 | 对电力企业造成重大的经济损失，或对大量公民、法人或其它组织的利益造成特别严重 |

| | | | |
|---|---|---|---|
| | 的损害。 | | 的损害。 |
| 社会秩序、公共利益 | 使电力生产及供应面临明显的中断威胁，影响波及一个地市的部分地区，对公众利益造成一定危害，可能扰乱社会秩序。 | 使电力生产及供应面临严重的中断威胁，影响波及一个或多个地市的部分地区，对公众利益造成严重危害，对社会秩序造成一定的影响。 | 使电网瓦解，发电机组停运，用电服务中断，影响波及一个或多个地市的大部分地区，严重扰乱社会秩序，对电力行业造成巨大经济损失，对公众利益造成特别严重危害。 |
| 国家安全 | 使电网瓦解，发电机组停运，电力生产与供应中断，影响波及一个或多个地市的部分地区，明显影响社会安定。 | 使电网瓦解，发电机组停运，电力生产与供应中断，影响波及一个或多个地市的大部分地区，对社会安定造成了严重的影响，明显影响国家安全。 | 造成电网瓦解，发电机组停运，电力生产与供应中断，影响波及一个或多个省市的大部分地区，引起社会动荡，严重威胁国家安全。 |

表 3 电力行业各类等级保护对象受破坏后可能侵害的客体与侵害程度

| 等级保护对象类别 | 可能侵害的客体与侵害程度 | | |
|---|---|---|---|
| | 其他公民、法人和组织的合法权益 | 社会秩序、公共利益 | 国家安全 |
| 电力监控系统 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害 |
| 管理信息系统 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害 |
| 通信网络设施 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害 | 一般损害 |
| 数据资源 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害 |
| 其他系统平台 | 一般损害<br>严重损害<br>特别严重损害 | 一般损害<br>严重损害 | —— |

电力企业可参照表 2 和表 3，结合定级对象的具体情况，从系统服务安全和业务信息安全两方面，具体分析定级对象受破坏后，可

能侵害的客体及其侵害程度。

（五）综合判定安全保护等级

根据业务信息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4可得到业务信息安全保护等级（S）。

表4 业务信息安全保护等级矩阵表

| 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 |
| 其他公民、法人和组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 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5可得到系统服务安全保护等级（A）。

表5 系统服务安全保护等级矩阵表

| 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 |
| 其他公民、法人和组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 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（S）和系统服务安全保护等级（A）的较高者决定，如表6所示。

表6 可能的定级情形

| 业务信息安全保护等级（S） | 系统服务安全保护等级（A） | 定级对象的安全保护等级 |
|---|---|---|
| 第一级 | 第一级 | 第一级 |
| 第二级 | 第一级 | 第二级 |
| 第一级 | 第二级 | |
| 第二级 | 第二级 | |
| 第三级 | 第一级或第二级 | 第三级 |
| 第一级或第二级 | 第三级 | |
| 第三级 | 第三级 | |

| | | |
|---|---|---|
| 第四级 | 第一级或第二级<br>或第三级 | 第四级 |
| 第一级或第二级<br>或第三级 | 第四级 | |
| 第四级 | 第四级 | |
| 第五级 | 第一级或第二级<br>或第三级或第四级 | 第五级 |
| 第一级或第二级<br>或第三级或第四级 | 第五级 | |
| 第五级 | 第五级 | |

（六）特殊对象的定级要求

对于通信网络设施、云计算平台/系统等定级对象，需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，原则上不低于其承载的等级保护对象的安全保护等级。

对于数据资源，综合考虑其规模、价值等因素，及其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侵害程度确定其安全保护等级。涉及大量公民个人信息以及为公民提供公共服务的大数据平台/系统，原则上其安全保护等级不低于第三级。

（七）等级变更

当等级保护对象所处理的业务信息和系统服务范围发生变化，可能导致业务信息安全或系统服务安全受到破坏后的受侵害客体和对客体的侵害程度发生变化时，需重新确定定级对象和安全保护等级。

## 六、电力行业重要等级保护对象定级建议

根据前述定级原理和方法，附件给出了电力行业部分重要等级

保护对象的定级建议。说明如下：

（1）附件给出了电力行业部分重要等级保护对象的建议等级。电力企业可根据具体情况分析本单位相关等级保护对象受到破坏时所侵害的客体及侵害程度，确定合适的安全保护等级。一般情况下，定级不应低于附件给出的建议等级。

（2）附件给出了电力行业一些典型的等级保护对象及其定级建议。对未列出的等级保护对象，电力企业可根据本指南给出的定级方法，参考附件中类似等级保护对象进行定级。

（3）附件给出了大数据平台和云计算平台的定级建议。平台的实际定级还需要考虑其上部署系统的定级情况，平台定级不得低于其上部署系统的安全保护等级。

附件：电力行业重要等级保护对象定级建议

附件

# 电力行业重要等级保护对象定级建议

| 类别 | 系统名称 | 范围 | 建议等级 | | |
|---|---|---|---|---|---|
| | | | 安全保护等级 | 业务信息安全保护等级 | 系统服务安全保护等级 |
| 电力监控系统 | 能量管理系统 | 省级及以上，具有SCADA、AGC、AVC等控制功能的系统 | 4 | 3 | 4 |
| | | 省级以下，具有SCADA、AGC、AVC等控制功能的系统 | 3 | 2 | 3 |
| | 变电站（含开关站、换流站、集控站）自动化系统 | 220千伏及以上，未作为调度自动化系统子站统一定级的系统 | 3 | 2 | 3 |
| | | 220千伏以下，未作为调度自动化系统子站统一定级的系统 | 2 | 2 | 2 |
| | 火电厂监控（含燃气电厂）系统DCS（含辅机控制系统） | 单机容量300兆瓦及以上 | 3 | 2 | 3 |
| | | 单机容量300兆瓦以下 | 2 | 2 | 2 |
| | 水电厂监控系统 | 总装机1000兆瓦及以上 | 3 | 2 | 3 |
| | | 总装机1000兆瓦以下 | 2 | 2 | 2 |
| | 水电厂梯级调度监控系统 | | 3 | 2 | 3 |
| | 核电站监控系统DCS（含辅机控制系统） | | 3 | 2 | 3 |
| | 风电场监控系统 | 总装机200兆瓦及以上 | 3 | 2 | 3 |
| | | 总装机200兆瓦以下 | 2 | 2 | 2 |
| | 光伏电站监控系统 | 总装机200兆瓦及以上 | 3 | 2 | 3 |
| | | 总装机200兆瓦以下 | 2 | 2 | 2 |
| | 风电场/光伏电站区域集控系统 | 总装机200兆瓦及以上 | 3 | 2 | 3 |
| | | 总装机200兆瓦以下 | 2 | 2 | 2 |
| | 电能量计量系统 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |
| | 广域相量测量系统（WAMS） | 省级及以上 | 3 | 2 | 3 |
| | 电网动态预警系统 | 省级及以上 | 3 | 2 | 3 |

| 类别 | 系统名称 | 范围 | 建议等级 | | |
|---|---|---|---|---|---|
| | | | 安全保护等级 | 业务信息安全保护等级 | 系统服务安全保护等级 |
| | 调度交易计划系统 | 省级及以上 | 3 | 2 | 3 |
| | 水调自动化系统 | | 2 | 2 | 2 |
| | 调度管理系统 | | 2 | 2 | 2 |
| | 雷电监测系统 | | 2 | 2 | 2 |
| | 核电站环境监测系统 | | 2 | 2 | 2 |
| | 核电站实物保护系统 | | 3 | 2 | 3 |
| | 风/光伏功率预测系统 | | 2 | 2 | 2 |
| | 新能源气象监测/信息系统 | | 2 | 2 | 2 |
| | 分布式电源集中控制系统 | | 2 | 2 | 2 |
| | 故障录波信息管理系统 | 调控中心侧系统 | 3 | 2 | 3 |
| | 配电监控系统 | | 3 | 2 | 3 |
| | 负荷控制管理系统 | | 3 | 2 | 3 |
| | 电力调度数据网络通信设备网管系统 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |
| | 电力调度数据网络通信资源管理系统 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |
| | 新一代电网调度控制系统的实时监控与预警功能模块 | 省级及以上 | 4 | 3 | 4 |
| | | 省级以下 | 3 | 2 | 3 |
| | 新一代电网调度控制系统的调度计划功能模块 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |
| | 新一代电网调度控制系统的安全校核功能模块 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |
| | 新一代电网调度控制系统的调度管理功能模块 | | 2 | 2 | 2 |
| 管理信息系统 | 企业对外门户网站系统 | 集团公司本部 | 3 | 3 | 3 |
| | | 二级公司及以下 | 2 | 2 | 2 |
| | 企业内部门户网站系统 | | 2 | 2 | 2 |
| | 95598 客户服务系统 | 全国范围系统 | 3 | 3 | 3 |
| | | 省级范围系统 | 2 | 2 | 2 |
| | 电动汽车充换电业务运营系统 | 用户规模 10 万以上 | 3 | 3 | 3 |
| | | 用户规模 10 万以下 | 2 | 2 | 2 |
| | 招投标管理系统 | 集团公司本部 | 3 | 3 | 3 |
| | | 二级公司及以下 | 2 | 2 | 2 |

| 类别 | 系统名称 | 范围 | 建议等级 | | |
|---|---|---|---|---|---|
| | | | 安全保护等级 | 业务信息安全保护等级 | 系统服务安全保护等级 |
| | 生产管理信息系统 | | 2 | 2 | 2 |
| | 电力市场信息系统 | 跨区跨省的电力实时交易 | 3 | 3 | 3 |
| | | 其他 | 2 | 2 | 2 |
| | 办公自动化（OA）系统 | 集团公司本部 | 3 | 3 | 3 |
| | | 二级公司及以下 | 2 | 2 | 2 |
| | 财务（资金）管理系统 | 集团公司本部、二级公司 | 3 | 3 | 3 |
| | | 二级公司以下 | 2 | 2 | 2 |
| | 人力资源管理系统 | 用户个人信息超10万条 | 3 | 3 | 2 |
| | | 用户个人信息不到10万条 | 2 | 2 | 2 |
| | 营销管理系统 | 集团公司本部、二级公司 | 3 | 3 | 3 |
| | | 二级公司以下 | 2 | 2 | 2 |
| | ERP 系统 | 集团公司本部、二级公司 | 3 | 3 | 3 |
| | | 二级公司以下 | 2 | 2 | 2 |
| | 物资管理系统 | | 2 | 2 | 2 |
| | 项目管理系统 | | 2 | 2 | 2 |
| | 邮件系统 | 集团公司级部署系统 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署系统 | 2 | 2 | 2 |
| | 即时通讯系统 | 集团公司级部署系统 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署系统 | 2 | 2 | 2 |
| | 修造管理信息系统 | | 2 | 2 | 2 |
| | 施工管理信息系统 | | 2 | 2 | 2 |
| | 大坝安全管理系统 | | 2 | 2 | 2 |
| | 电力设计管理信息系统 | 二级公司（或甲级资质）及以上设计单位 | 3 | 3 | 3 |
| | | 二级公司（或甲级资质）以下设计单位 | 2 | 2 | 2 |
| | 电力监管信息系统 | | 3 | 3 | 3 |
| 通信网络 | 电力调度数据网络 | 省级及以上 | 3 | 2 | 3 |
| | | 省级以下 | 2 | 2 | 2 |

| 类别 | 系统名称 | 范围 | 建议等级 | | |
|---|---|---|---|---|---|
| | | | 安全保护等级 | 业务信息安全保护等级 | 系统服务安全保护等级 |
| 设施 | 电力企业广域网 | | 2 | 2 | 2 |
| | 电力监管广域网 | | 2 | 2 | 2 |
| | 综合数据通信网络 | | 2 | 2 | 2 |
| 数据资源 | 大数据平台 | 集团公司级部署平台 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署平台 | 2 | 2 | 2 |
| 其他系统平台 | 云计算平台 | 集团公司级部署平台 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署平台 | 2 | 2 | 2 |
| | 统一身份认证系统 | 集团公司级部署平台 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署平台 | 2 | 2 | 2 |
| | 物联网平台 | 集团公司级部署系统 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署系统 | 2 | 2 | 2 |
| | 网络安全态势感知平台 | 集团公司级部署系统 | 3 | 3 | 3 |
| | | 二级公司及以下单位独立部署系统 | 2 | 2 | 2 |

国家能源局综合司　　2022年7月19日印发