**ICS 19.020**

|  |
| --- |
| **CCS K85** |

CSEE

团体标准

T/CSEE XXXX-YYYY

|  |
| --- |
|  |

电力物联网数据安全分级及管控要求

|  |
| --- |
| Technical Requirements for Power IoT Data Security Classification  （征求意见稿） |

XXXX - XX - XX发布

XXXX - XX - XX实施

中国电机工程学会   发 布

目  次

[前  言 II](#_Toc31554)

[1 范围 1](#_Toc4649)

[2 规范性引用文件 1](#_Toc7604)

[3 术语和定义 1](#_Toc2931)

[4 适用数据范围 2](#_Toc21202)

[5 数据分级及管控前提条件 2](#_Toc441)

[5.1 建立组织保障 2](#_Toc3267)

[5.2 建立管理制度 2](#_Toc18649)

[5.3 建立数据资产清单 2](#_Toc20390)

[6 数据分级 2](#_Toc20988)

[6.1 数据分级原则 2](#_Toc28407)

[6.2 数据分级要点 3](#_Toc13187)

[6.3 数据分级方法 3](#_Toc15635)

[6.3.1数据定级要素 3](#_Toc23991)

[6.3.2数据等级描述标识 5](#_Toc15105)

[6.3.3数据特征描述 5](#_Toc16374)

[6.3.4数据定级流程 6](#_Toc2890)

[6.3.5等级变更 9](#_Toc18599)

前  言

本文件按照《中国电机工程学会标准管理办法（暂行）》的要求，依据GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》给出的规则起草。

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专利的责任。

本文件由中国电机工程学会提出。

本文件由中国电机工程学会电力信息化专业委员会技术归口和解释。

本文件起草单位：中国电力科学研究院有限公司、国网黑龙江省电力有限公司电力科学研究院、国网山东信通公司、国网吉林信通公司

本文件主要起草人：

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国电机工程学会标准执行办公室（地址：北京市西城区白广路二条1 号，100761，网址：http：//www.csee.org.cn，邮箱：cseebz@csee.org.cn）。

电力物联网数据安全分级及管控要求

1. 范围

本标准内容主要针对电力物联网数据实施分级而提出的指导方法。参考国内外相关标准，明确电力物联网数据分级的原则，在该原则的指导下，根据数据管理及开放过程中安全属性（完整性、保密性、可用性）遭到破坏后可能的影响程度对各类数据所属详细子项进行定级，共分为四级。

涉及国家秘密的数据需遵从国家有关规定，不在本指南中详述。

1. 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/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

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GA/T 1389-2017 信息安全技术 网络安全等级保护定级指南

XXXX—XXXX 工业数据分类分级指南（试行）

1. 术语和定义

GB/T25069-2010界定的以及下列术语和定义适用于本文件。

3.1.1

电力物联网 power Internet of things

应用于电网的工业级物联网，在线连接能源生产、传输与消费各环节的人、机、物。

3.1.2

影响对象 influence object

数据安全性遭受破坏后受到影响的对象类型，可划分为客户/个人，社会秩序/公共利益，国家安全。

3.1.3  
影响范围 sphere of influence

数据安全性遭受破坏后所产生影响的边界，可划分机构，企业，行业。

1. 适用数据范围

本标准适用于电力物联网经营和管理活动中产生、采集、加工、使用或管理的数据，包括但不限于以下：电力数据包括电力系统、设备数据、电能数据、电量数据、电价数据等；通用数据包括客户数据、交易数据、综合数据等；基础数据包括标准数据、章程数据等。

1. 数据分级前提条件

5.1 建立组织保障

数据分级工作的开展需要有组织保障，明确：

1. 数据分级的管理部门；
2. 数据分级的最高责任人；
3. 数据分级相关的管理角色和职能；
4. 数据分级相关的授权机制。

5.2 建立管理制度

数据分级工作的开展需要有制度保障，明确：

1. 数据分级的具体要求；
2. 数据分级工作中涉及的角色及职责；
3. 数据分级的相关制度和操作流程的制定、发布、维护和更新的机制以及评审和修订周期；
4. 数据分级管理相关绩效考评和评价机制；
5. 数据分级的原则、方法；
6. 数据级别的相关变更原则及变更后的通知原则；
7. 数据资产分级清单的审核与修订周期和原则；
8. 数据分级保护的总体原则和目标；
9. 数据分级的日常管理流程；
10. 操作人员的操作规程。

5.3 建立数据资产清单

至少采取以下措施，有效管理数据资产：

1. 收集所有生产、采集、加工、使用或管理的数据，对数据进行明确的定义，并根据数据分级方法对数据进行分级并标识，建立数据资产分级清单；
2. 数据资产分级清单的内容宜经数据管理相关方评审确认；
3. 对数据资产分级清单进行定期修订。
4. 数据分级

6.1 数据分级原则

数据分级宜遵循以下原则：

1. 依从性原则：数据级别划分应满足相关法律、法规及监管要求；
2. 可执行性原则：宜避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性；
3. 时效性原则：数据的分级具有一定的有效期。数据的级别可能因时间变化按照一些预定的安全策略发生改变；
4. 自主性原则：机构可根据自身的数据管理需要，例如战略需要、业务需要、对风险的接受程度等，按照数据分级方法自主确定更多的数据层级，并为数据定级，但不宜将高敏感度数据定为低敏感度级别；
5. 合理性原则：数据级别宜具有合理性，不能将所有数据集中划分一两个级别中，而另外一些没有数据。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支；
6. 客观性原则：数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级，已经分级的数据是可以复核和检查的。

6.2 数据分级要点

数据分级工作中，注意以下方面:

1. 对数据泄露或损坏影响宜基于数据完全泄露或损坏来考虑，而不宜基于已有任何技术的防护措施来考虑；
2. 《中国人民共和国网络安全法》已明确要对个人信息保护，要高度重视用户或业务相关的个人信息保护，在数据分级中从高考虑；
3. 安全属性（完整性、保密性、可用性）是信息安全风险评估中的重要参考属性，针对数据分级，数据安全属性遭到破坏后可能造成的影响，是确定数据级别的重要判断依据，推荐采用。

6.3 数据分级方法

6.3.1数据定级要素

数据定级六要素如下：

1. 影响对象，划分为：客户/个人，社会秩序/公共利益，国家安全；
2. 影响范围，划分为：机构，企业，行业；
3. 影响程度，一般指数据安全属性（完整性、保密性、可用性）遭到破坏后带来的影响大小。划分为：非常严重、严重、中等、轻微；
4. 与生产业务关联性，依据《工业数据分类分级指南》，划分为：一级，二级，三级；
5. 业务系统关联性，依据《信息系统安全等级保护定级指南》中业务信息安全保护等级，划分为：一级，二级，三级，四级，五级。

6.3.1.1关于影响对象的说明

影响对象的确定应考虑以下内容：

1. 影响对象为国家安全的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对国家安全造成影响，包括以下几方面：
2. 影响国家政权稳固和国防实力；
3. 影响国家统一、民族团结和社会安定；
4. 影响国际对外活动中的政治经济利益；
5. 影响国家经济竞争力和科技实力；
6. 其它影响国家安全的事项。
7. 影响对象为社会秩序/公共利益的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对社会秩序/公共利益造成影响。侵害社会秩序的事项包括以下几方面：
8. 影响国家机关社会管理和公共服务的工作秩序；
9. 影响各种类型的经济活动秩序；
10. 影响各行业的科研、生产秩序；
11. 影响公众在法律约束和道德规范下的正常生活秩序等；
12. 其他影响社会秩序的事项。

侵害公共利益的事项包括以下方面：

1. 影响社会成员使用公共设施；
2. 影响社会成员获取公开信息资源；
3. 影响社会成员接受公共服务等方面；
4. 其他影响公共利益的事项。
5. 影响对象为客户/个人的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对公民、法人、组织的社会权益、经济利益等造成影响。

6.3.1.2关于影响范围的说明

影响范围的确定应考虑以下内容：

1. 影响范围为机构的情况，是指数据的安全性遭到破坏后，所造成的影响仅限于本机构范围内的情形；
2. 影响范围为企业的情况，是指数据的安全性遭到破坏后，所造成的影响仅限于本公司范围内的情形；
3. 影响范围为行业的情况，是指数据的安全性遭到破坏后，可能会对电力行业及其他行业中一个或多个行业造成的影响的情形。

6.3.1.3关于影响程度的说明

影响程度的判定，宜综合考虑数据类型特征。数据类型根据业务条线划分并确定，不同业务对应不同的数据类型，体现不同的业务特点。为便于确定影响程度，下表提供影响程度的参考说明，供判定影响程度时参考。

表1 影响程度说明

|  |  |
| --- | --- |
| 影响程度 | 参考说明 |
| 非常严重 | 1、导致全部业务无法开展，造成重大经济损失。  2、出现极其严重的法律问题，大范围的社会不良影响。  3、对其他组织和个人造成非常严重损害。 |
| 严重 | 1、导致部分业务无法开展，造成较大经济损失。  2、出现严重的法律问题，一定范围的社会不良影响。  3、对其他组织和个人造成严重损害。 |
| 中等 | 1、影响业务正常开展，造成一定经济损失。  2、出现法律问题，对社会造成不良影响。  3、对其他组织和个人造成损害。 |
| 轻微 | 1、对业务正常开展造成轻微影响，造成轻微经济损失。  2、对社会造成轻微影响。  3、对其他组织和个人造成轻微损害。 |

6.3.1.4关于与生产业务关联性的说明

与生产业务关联性的判定依据是《工业数据分类分级指南》中的划分原则，划分为：一级数据，二级数据，三级数据。

1. 潜在影响符合下列条件之一的数据为三级数据：
2. 易引发特别重大生产安全事故或突发环境事件，或造成直接经济损失特别巨大；
3. 对国民经济、行业发展、公众利益、社会秩序乃至国家安全造成严重影响。
4. 潜在影响符合下列条件之一的数据为二级数据：
5. 易引发较大或重大生产安全事故或突发环境事件，给企业造成较大负面影响，或直接经济损失较大；
6. 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或影响持续时间长，或可导致大量供应商、客户资源被非法获取或大量个人信息泄露；
7. 恢复工业数据或消除负面影响所需付出的代价较大。
8. 潜在影响符合下列条件之一的数据为一级数据：
9. 对工业控制系统及设备、工业互联网平台等的正常生产运行影响较小；
10. 给企业造成负面影响较小，或直接经济损失较小；
11. 恢复工业数据或消除负面影响所需付出的代价较小。

6.3.1.5关于与业务系统关联性的说明

与业务系统关联性，依据是《信息系统安全等级保护定级指南》中业务信息安全保护等级的划分原则，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，得到业务信息安全保护等级，如表2所示。

表2 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 |
| 公民、法人和其他组织的合法权益 | 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 |

6.3.2数据等级描述标识

数据定级一般使用等级描述标识进行描述。

本指南中的数据等级分为四级，描述标识分为数据级别标识和数据重要程度标识两类，相互一一对应。

1. 数据级别标识，从高到低划分为：四级、三级、二级、一级。
2. 数据重要程度标识，与数据级别标识相对应，从高到低划分为：极高、高、中、低。

6.3.3数据特征描述

数据级别从高到低，一般具有如下数据特征：

1. 四级（极高）：数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。
2. 三级（高）：数据用于重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。
3. 二级（中）：数据用于一般业务使用，一般针对受限对象公开；一般指内部管理且不宜广泛公开的数据。
4. 一级（低）：数据一般可被公开或可被公众获知、使用。

注：“必须知悉”是指对数据确定知悉范围，只有对数据知悉有明确的必要性时，该对象才能对数据知悉。一般情况下遵循工作需要原则和最小化原则，前者指因工作需要才可知悉，后者指知悉的范围尽可能小。

关于数据特征的说明:

1. 数据特征中所指的数据内容可公开的范围、对象、与生产业务相关性、与业务系统相关性需由各机构自行指定。
2. 数据级别确定中，需综合考虑数据安全属性（完整性、保密性、可用性）因素。在完整性和可用性要求基本一致情况下，宜重点以敏感性为定级依据。此外，经综合分析后，允许存在数据内容面向公众公开，但完整性或可用性要求高，最终确定的数据级别应选取较高的情况。

6.3.4数据定级流程

本指南中的数据定级分为五个个步骤，分别是常规定级流程、由与生产业务关联性定级、由与业务系统关联性定级及最终定级。数据定级流程图如下图所示：

图1 定级流程图

6.3.4.1常规定级流程

常规定级流程应遵循以下步骤：

1. 确定影响对象。确定需定级的某类数据的安全属性（完整性、保密性、可用性）遭到破坏后可能影响的对象，包括客户/个人、社会秩序/公共利益、国家安全。
2. 确定影响范围。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响的范围，包括客机构，企业，行业。
3. 确定影响程度。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响程度，包括非常严重、严重、中等、轻微。
4. 确定数据定级。数据安全级别划定规则如表3所示。

表3 数据安全常规定级规则参考表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 数据定级要素 | | | 数据一般特征 | 数据重要程度标识 | 数据级别标识 |
| 影响对象 | 影响范围 | 影响程度 |
| K/S/G | 行业 | 非常严重 | 1、数据安全性遭到破坏后，影响国家安全、社会和电力市场稳定，或影响范围为多行业或电力行业内多个机构，影响程度一般是“非常严重”。  2、只针对特定人员公开，且仅为必须知悉的对象访问或使用。 | 极高 | 四级 |
| K/S/G | 行业 | 严重 |
| G | 企业 | 非常严重 |
| S | 企业 | 非常严重 |
| K | 企业 | 非常严重 |
| K | 机构 | 非常严重 |
| K/S/G | 行业 | 中等 | 1、数据的安全性遭到破坏后，影响范围一般为电力行业内多个机构或本机构，影响程度一般是“严重”。  2、数据用于重要业务使用，针对特定人员公开，且仅为必须知悉的对象访问或使用。 | 高 | 三级 |
| G | 企业 | 严重 |
| S | 企业 | 严重 |
| S | 机构 | 非常严重 |
| S | 机构 | 严重 |
| K | 企业 | 严重 |
| K | 机构 | 严重 |
| K/S/G | 行业 | 轻微 | 1、数据的安全性遭到破坏后，影响范围一般局限在本机构，影响程度一般是“中等”。  2、数据用于一般业务使用，针对受限对象公开；一般指内部管理、办公类且不宜广泛公开的数据。 | 中 | 二级 |
| G | 企业 | 中等 |
| S | 企业 | 中等 |
| S | 机构 | 中等 |
| K | 企业 | 中等 |
| K | 机构 | 中等 |
| G | 企业 | 轻微 | 1、数据的安全性遭到破坏后数据损失后，影响范围一般局限在本机构，影响程度一般是“轻微”或“无”。  2、数据可被公开或可被公众获知、使用。 | 低 | 一级 |
| S | 企业 | 轻微 |
| S | 机构 | 轻微 |
| H | 企业 | 轻微 |
| H | 机构 | 轻微 |

注：K 表示客户/个人、S 表示社会秩序/公共利益、G 表示国家安全

6.3.4.2由与生产业务关联性定级

由与生产业务关联性定级流程应遵循以下步骤：

1. 依据《工业数据分类分级指南》，确定数据的工业数据等级。
2. 确定影响程度。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响程度，包括非常严重、严重、中等、轻微。
3. 确定数据定级。根据数据的工业数据等级和影响程度确定数据的安全级别，划定规则如表5所示。

表5 由与生产业务关联性定级规则参考表

|  |  |  |  |
| --- | --- | --- | --- |
| 数据定级要素 | | 数据重要程度标识 | 数据级别标识 |
| 工业数据等级 | 影响程度 |
| 三级/二级 | 非常严重 | 极高 | 四级 |
| 三级 | 严重 |
| 三级 | 中等 | 高 | 三级 |
| 二级 | 严重 |
| 一级 | 非常严重 |
| 三级 | 轻微 | 中 | 二级 |
| 二级 | 中等 |
| 一级 | 严重/中等 |
| 二级 | 轻微 | 低 | 一级 |
| 一级 | 轻微 |

6.3.4.3由与业务系统关联性定级

由与业务系统关联性定级流程应遵循以下步骤：

1. 依据《信息系统安全等级保护定级指南》，确定数据的业务信息安全等级。
2. 确定影响程度。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响程度，包括非常严重、严重、中等、轻微。
3. 确定数据定级。根据数据的业务信息安全等级和影响程度确定数据的安全级别，划定规则如表6所示。

表6 由与业务系统关联性定级规则参考表

|  |  |  |  |
| --- | --- | --- | --- |
| 数据定级要素 | | 数据重要程度标识 | 数据级别标识 |
| 业务信息安全等级 | 影响程度 |
| 五级/四级/三级 | 非常严重 | 极高 | 四级 |
| 五级 | 严重 |
| 五级 | 中等 | 高 | 三级 |
| 四级/三级 | 严重 |
| 二级 | 非常严重 |
| 五级 | 轻微 | 中 | 二级 |
| 四级/三级 | 中等 |
| 二级 | 严重/中等 |
| 一级 | 非常严重/严重 |
| 四级/三级/二级 | 轻微 | 低 | 一级 |
| 一级 | 中等/轻微 |

6.3.4.4最终定级

定级对象的安全保护等级服从就高原则，即定级对象的安全保护等级由常规定级、由与生产业务相关性定级和由与业务系统相关性定级中级别最高的级数确定。

6.3.5等级变更

在对数据进行管理过程中，为避免数据安全受到威胁时，对公司造成较大的危害程度，应根据本章给出的定级方法重新定级。