|  |  |
| --- | --- |
| ICS | 点击此处添加ICS号 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png CECS |   点击此处添加CCS号 |

中国工程建设标准化协会团体标准

T/CECS XXXX—202X

油气管网工业控制系统

网络安全等级保护定级

Classification guide for classified protection of cybersecurity

for Industrial control system of oil and gas pipeline network

202X - XX - XX发布

202X - XX - XX实施

中国工程建设标准化协会  发布

目次

[前言 III](#_Toc198744390)

[1 范围 1](#_Toc198744391)

[2 规范性引用文件 1](#_Toc198744392)

[3 术语和定义 1](#_Toc198744393)

[4 定级原则 2](#_Toc198744399)

[4.1 合规性原则 2](#_Toc198744400)

[4.2 按类归并原则 2](#_Toc198744401)

[4.3 保护等级最高原则 2](#_Toc198744402)

[5 定级原理与流程 2](#_Toc198744403)

[5.1 定级原理 2](#_Toc198744404)

[5.2 定级要素 2](#_Toc198744405)

[6 定级对象 5](#_Toc198744406)

[6.1 要素划分 5](#_Toc198744407)

[6.2 工控系统风险等级 5](#_Toc198744408)

[7 定级方法 5](#_Toc198744409)

[7.1 定级方法 5](#_Toc198744410)

[7.2 系统服务安全保护等级的确定 6](#_Toc198744411)

[7.3 专家评审 7](#_Toc198744412)

[7.4 上级审批 7](#_Toc198744413)

[7.5 系统备案 7](#_Toc198744414)

[8 等级变更 7](#_Toc198744415)

[附录A （资料性） 网络安全等级保护定级报告模板 8](#_Toc198744416)

[附录B （资料性） 网络安全等级保护备案表模板 10](#_Toc198744420)

[参考文献 11](#_Toc198744421)

[图1 定级流程示意图 4](#_Toc198144347)

[表1 网络安全保护等级说明 2](#_Toc198744193)

[表2 受侵害程度判别基准 3](#_Toc198744194)

[表3 三种侵害程度描述 4](#_Toc198744195)

[表4 定级要素与网络安全保护等级的关系 4](#_Toc198744196)

[表5 业务信息遭到破坏时所侵害客体及对客体的侵害程度 6](#_Toc198744197)

[表6 业务信息安全保护等级确定 6](#_Toc198744198)

[表7 系统服务遭到破坏时所侵害客体及对客体的侵害程度 7](#_Toc198744199)

[表8 系统服务安全保护等级确定 7](#_Toc198744200)

[表A.1 业务信息安全等级表 8](#_Toc198744201)

[表A.2 系统服务安全等级表 9](#_Toc198744202)

[表A.3 系统安全保护等级表 9](#_Toc198744203)

[图B.1 网络安全等级保护备案表封面 10](#_Toc198744204)

1. 前言

本文件按照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》的规定起草。

请注意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。

本文件由中国工程建设标准化协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

油气管网工业控制系统

网络安全等级保护定级

* 1. 范围

本文件给出了油气管网工业控制系统（以下简称“工控系统”）的网络安全保护等级的定级原则、定级原理、定级对象、定级流程和方法、专家评审、上级审批等要求。

本文件适用于工控系统运营者对安全等级保护的定级工作。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术术语

GB/T 26333-2010 工业控制网络安全风险评估规范

GB/T 29246-2017 信息安全 安全技术 信息安全管理体系 概述和词汇

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 35295-2017 信息技术 大数据 术语

GA 1166-2014 石油天然气管道系统治安风险等级和安全防范要求

* 1. 术语和定义

GB 17859-1999、GB/T 22239-2019、GB/T 22240-2020、GB/T 25069、GB/T 26333-2010、GB/T 29246-2017、GB/T 31167-2014、GB/T 32919-2016、GB/T 35295-2017和GA 1166-2014界定的以及下列术语和定义适用于本文件。

* + 1. 国家骨干管道 state main pipeline

承担石油、天然气输送，对国家经济社会影响重大，天然气年设计输气量大于等于100×108m3、原油年设计输量大于等于1000×104t、成品油年设计输量大于等于500×104t的长距离管道及跨国管段。

* + 1. 油气管网工业控制系统 industrial control system of oil and gas pipeline network

油气管网中用于数据采集、监视等功能的工业控制系统，包括油气管道SCADA系统、LNG接收站和储气库DCS系统。

* + 1. 客体 object

工控系统受到破坏时所侵害的社会关系。

* + 1. 系统服务 system service

工控系统为支撑其所承载业务而提供的程序化过程。

* + 1. 定级要素 grading elements

由受侵害的客体和对客体的侵害程度构成的要素。

* 1. 定级原则
     1. 合规性原则

作为等级保护对象的工控系统定级时需按照相关法律法规的要求合理定级。

* + 1. 按类归并原则

作为等级保护对象的工控系统需根据安全责任主体、业务类型、相同的物理位置或相似的运行环境等方面进行归类。

* + 1. 保护等级最高原则

如果等级保护对象承载多项业务功能和数据，则该等级保护对象的网络安全保护等级需由最关键业务功能和数据所决定。

* 1. 定级原理与流程
     1. 定级原理

1. 工控系统的网络安全保护等级按照相关要求[[1]](#footnote-1)1）分为五个安全等级，见表1。
2. 网络安全保护等级说明

| 网络安全保护等级 | 基本描述 |
| --- | --- |
| 第一级 | 等级保护对象受到破坏后，会对相关公民、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 | 等级保护对象受到破坏后，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 | 等级保护对象受到破坏后，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 | 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危害，或者对国家安全造成严重危害。 |
| 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危害。 |

* + 1. 定级要素
       1. 定级要素概述

等级保护对象受到破坏时所侵害的客体应包括以下三个方面：

1. 国家安全；
2. 社会秩序、公共利益；
3. 公民、法人和其他组织的合法权益。

侵害不同客体的事项是不同的,具体包括：

1. 侵害国家安全的事项包括：
   1. 影响国家政权稳固和领土主权、海洋权益完整；
   2. 影响国家统一、民族团结和社会稳定；
   3. 影响国家社会主义市场经济秩序和文化实力；
   4. 其他影响国家安全的事项。
2. 侵害社会秩序的事项包括：
   1. 影响国家机关、企事业单位、社会团体的生产秩序、经营秩序等；
   2. 影响公共场所的活动秩序、公共交通秩序；
   3. 影响人民群众的生活秩序；
   4. 其他影响社会秩序的事项。
3. 侵害公共利益的事项包括：
   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。
4. 侵害公民、法人和其他组织的合法权益是指由受法律保护的公民、法人和其他组织所享有的社会权利和利益等受到损害。

确定受侵害的客体时，宜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。

* + - 1. 对客体的侵害程度

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。

对客体的侵害外在表现为对等级保护对象的破坏，其危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内信息的机密性、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。
   * + 1. 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，首先根据不同的受侵害客体、不同危害后果分别确定其侵害程度。对不同侵害后果确定其危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网络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。

在针对不同的受侵害客体进行侵害程度的判断时，宜参照不同的判别基准，受侵害程度判别基准见表2。

1. 受侵害程度判别基准

| 受侵害的客体 | 受侵害程度判别基准 |
| --- | --- |
| 公民、法人或其他组织的合法权益 | 以本人或本单位的总体利益作为判断侵害程度的基准 |
| 社会秩序、公共利益或国家安全 | 以整个行业或国家的总体利益作为判断侵害程度的基准 |

不同侵害后果的三种侵害程度描述见表3。

1. 三种侵害程度描述

| 危害程度 | 具体描述a |
| --- | --- |
| 一般损害 | 发生一般生产安全事故或一般环境事件时的影响。 |
| 严重损害 | 发生较大生产安全事故或较大环境事件时的影响。 |
| 特别严重损害 | 发生重大/特别重大生产安全事故或重大/特别重大环境事件时的影响。 |

* + - 1. 定级要素与网络安全保护等级的关系

定级要素与网络安全保护等级的关系见表4。

1. 定级要素与网络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 |
| 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 |

* + - 1. 定级流程

工控系统的定级流程示意图见图1。



1. 定级流程示意图

工控系统网络安全保护等级的确定首先应对定级对象的定级要素进行分析，然后分别得出业务信息安全等级和系统服务安全等级，最后综合确定出定级对象的网络安全保护等级。

* 1. 定级对象
     1. 要素划分

工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。现场采集/执行、现场控制和过程控制等要素应作为一个整体对象定级，生产管理要素宜单独定级。

* + 1. 工控系统风险等级
       1. 一级风险工业控制系统

一旦遭受侵害，将导致油气管网大范围停产、停供，或易引发闪燃、爆炸、严重环境污染等次生灾害，造成特大人员伤亡或巨额财产损失，引起重大社会公众恐慌的工业控制系统。一级风险工业控制系统主要包括：

1. 国家油气调控中心的工业控制系统；
2. 省级和区域控制中心的工业控制系统；
3. 国家战略储油库、储气库和LNG接收站的工业控制系统；
4. 国家骨干管道的首站、末站和枢纽站的工业控制系统；
5. 位于治安复杂区域或人口密集区域的国家骨干管道系统的工业控制系统；
6. 其他经网络安全风险分析可被评定为一级风险的工业控制系统。
   * + 1. 二级风险工业控制系统

一旦遭受侵害，将对油气管网系统造成较大范围的停产、停供，或可能引发闪燃、爆炸、严重环境污染等次生灾害，导致重大人员伤亡或财产损失的工业控制系统。二级风险工业控制系统主要包括：

1. 国家骨干管道的加压站、减压站、输油站、输气站的工业控制系统；
2. 非国家战略级的储油库、储气库和LNG接收站的工业控制系统；
3. 非国家骨干管道系统的首站和末站的工业控制系统；
4. 位于治安复杂区域或人口密集区域的非国家骨干管道系统的工业控制系统；
5. 其他经网络安全风险分析可被评定为二级风险的工业控制系统。
   * + 1. 三级风险工业控制系统

除一级、二级风险工业控制系统以外的站场、阀室的工业控制系统，可能造成局部停产、停供，对油气管网运行造成有限影响的工业控制系统。

* 1. 定级方法
     1. 定级方法
        1. 业务信息安全保护等级的确定

工控系统的业务信息主要包括工况参数、工艺参数、设备运行参数、控制/联锁回路信息、其他可能影响国家安全的参数等。

1. 工况参数主要为站场压力、温度等参数。
2. 工艺参数主要为压缩机、流量计、分析仪、阀门等的工艺参数。
3. 设备运行参数主要为电气设备、控制设备等的运行状态相关参数。
4. 控制/联锁回路信息是指工控系统在运行过程中为达到期望的控制效果而发出的控制指令，以实现数据测量、设备控制、参数调节等功能的联锁参数。
5. 其他可能影响国家安全的数据主要包括油气输送量、站场经纬度等相关信息。

这些业务信息遭到破坏（被非法窃取、篡改和不可用）后，可能会导致管道生产运行信息泄露、生产运行的远传数据不准确或无法及时反映生产运行情况，会造成生产集中监控局部失效等影响。工控系统业务信息遭到破坏时所侵害客体及对客体的侵害程度见表5。

1. 业务信息遭到破坏时所侵害客体及对客体的侵害程度

| 定级对象 | 受侵害的客体 | 对客体的侵害程度 | 业务信息分类 | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 工况参数 | 工艺参数 | 设备运行状态参数 | 控制/联锁回路信息a | 其他可能影响国家安全的数据 |
| 一级风险部位油气管网工业控制系统 | 公民、法人和其他组织的合法权益 | 一般损害 | × | × | × | × | × |
| 严重损害 | √ | √ | √ | √ | √ |
| 特别严重损害 | × | × | × | × | × |
| 社会秩序、公共利益 | 一般损害 | √ | √ | × | √ | √ |
| 严重损害 | × | × | × | √ | × |
| 特别严重损害 | × | × | × | × | × |
| 国家安全 | 一般损害 | × | × | × | × | √ |
| 严重损害 | × | × | × | × | × |
| 特别严重损害 | × | × | × | × | × |
| 二级风险部位油气管网工业控制系统 | 公民、法人和其他组织的合法权益 | 一般损害 | √ | √ | √ | √ | √ |
| 严重损害 | × | × | × | × | × |
| 特别严重损害 | × | × | × | × | × |
| 社会秩序、公共利益 | 一般损害 | **√** | **√** | **×** | **√** | **√** |
| 严重损害 | **×** | **×** | **×** | **×** | **×** |
| 特别严重损害 | **×** | **×** | **×** | **×** | **×** |
| 国家安全 | 一般损害 | **×** | **×** | **×** | **×** | **√** |
| 严重损害 | **×** | **×** | **×** | **×** | **×** |
| 特别严重损害 | **×** | **×** | **×** | **×** | **×** |
| 1. 当输送介质为气时，控制/联锁回路信息遭到破环对社会秩序、公共利益的侵害程度为一般损害；当输送介质为油时，控制/联锁回路信息遭到破环对社会秩序、公共利益的侵害程度为严重损害。油气管道的控制/联锁回路信息遭到破环对社会秩序、公共利益的侵害程度宜保持一致。 | | | | | | | |

根据业务信息遭到破坏时所侵害客体和对侵害客体的侵害程度，依据表6可得到业务信息安全保护等级。

1. 业务信息安全保护等级确定

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

* + 1. 系统服务安全保护等级的确定

工控系统的系统服务遭到破坏，主要包括系统服务暂停、系统服务终止、系统异动等情况，会导致生产实时数据采集、监视控制、生产调度不能正常进行，可能造成管道系统输量大范围波动和大范围停产、停供、设备损坏、管线破裂等，且易发生闪燃、闪爆、严重环境污染等次生灾害，导致人员伤亡或财产损失等。工控系统系统服务遭到破坏时所侵害客体及对客体的侵害程度见表7。

1. 系统服务遭到破坏时所侵害客体及对客体的侵害程度

| 定级对象 | 受侵害的客体 | 对客体的侵害程度 | 系统服务状态分类 | |
| --- | --- | --- | --- | --- |
| 系统服务停止 | 系统异动 |
| 一级风险部位油气管网工业控制系统 | 公民、法人和其他组织的合法权益 | 一般损害 | × | × |
| 严重损害 | √ | √ |
| 特别严重损害 | × | × |
| 社会秩序、公共利益 | 一般损害 | √ | × |
| 严重损害 | × | √ |
| 特别严重损害 | × | × |
| 国家安全 | 一般损害 | × | × |
| 严重损害 | × | × |
| 特别严重损害 | × | × |
| 二级风险部位油气管网工业控制系统 | 公民、法人和其他组织的合法权益 | 一般损害 | √ | √ |
| 严重损害 | × | × |
| 特别严重损害 | × | × |
| 社会秩序、公共利益 | 一般损害 | √ | √ |
| 严重损害 | × | × |
| 特别严重损害 | × | × |
| 国家安全 | 一般损害 | × | × |
| 严重损害 | × | × |
| 特别严重损害 | × | × |

根据系统服务遭到破坏时所侵害客体和对侵害客体的侵害程度，依据表8可得到业务信息安全保护等级。

1. 系统服务安全保护等级确定

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

确定安全保护定级

工控系统网络安全保护等级由业务信息安全等级和系统服务安全等级的较高者确定。

* + 1. 专家评审

定级对象确定为等级保护第二级及以上的工控系统需组织专家评审会。定级对象的运营、使用单位应组织网络安全专家和业务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。

* + 1. 上级审批

完成专家评审后，应将等级保护定级报告、等级保护备案表和专家评审意见等相关材料，报上级管理部门审核。经上级管理部门审核同意后，再报送公安机关备案。等级保护定级报告模板见附录A。

* + 1. 系统备案

等级保护第二级及以上的工控系统在网络安全保护等级确定后10个工作日内，由安全责任单位办理备案手续。办理备案手续时，需按照属地公安机关相关要求提供材料，包括但不限于等级保护定级报告、等级保护备案表和专家评审意见等材料。等级保护备案表模板见附录B。

* 1. 等级变更

当被定级的工控系统所处理的业务信息和系统服务范围发生变化，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，需根据本文件7.2给出的定级方法重新定级，并根据属地公安机关相关要求提交材料或重新备案。

1. （资料性）  
   网络安全等级保护定级报告模板
   1. XXX系统描述

简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担信息系统安全责任的XX单位XX部门，说明本XX单位XX部门对信息系统具有信息安全保护责任，该信息系统为XX单位XX部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务，业务情况描述。

* 1. 网络安全保护义务的责任落实

按照《网络安全法》的相关要求，此次备案的XX系统的网络安全保护义务由XX单位履行，日常网络安全工作由我单位XX部门负责落实，XX部门负责人（姓名、身份证号码）为直接负责的主管人员。

* 1. XXX系统安全保护等级确定
     1. 业务信息安全保护等级的确定
        1. 业务信息描述

描述信息系统处理的主要业务信息，信息量，采集频率，是否涉及个人信息或敏感信息。

* + - 1. 业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时（考虑丢失、篡改和泄露的不同破坏方式）侵害的客体是什么，即对三个客体（国家安全；社会秩序和公共利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

* + - 1. 信息受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

* + - 1. 业务信息安全等级的确定

依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级。

表A.1 业务信息安全等级表

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

* + 1. 系统服务安全保护等级的确定
       1. 系统服务描述

描述信息系统的服务范围、服务对象、服务连续性要求等。

* + - 1. 系统服务受到破坏时所侵害客体的确定

说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公共利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

* + - 1. 系统服务受到破坏后对侵害客体的侵害程度的确定

说明系统服务受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

* + - 1. 系统服务安全等级的确定

依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级。

表A.2 系统服务安全等级表

|  |  |  |  |
| --- | --- | --- | --- |
| 系统服务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 |

* + 1. 安全保护等级的确定

系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定XXX系统安全保护等级为第几级。

表A.3 系统安全保护等级表

|  |  |  |  |
| --- | --- | --- | --- |
| 系统名称 | 安全保护等级 | 业务信息安全等级 | 系统服务安全等级 |
| XXX系统 | X | X | X |

1. （资料性）  
   网络安全等级保护备案表模板



图B.1 网络安全等级保护备案表封面

参考文献

[1] 中华人民共和国网络安全法

[2] 中华人民共和国数据安全法

[3] 关键信息基础设施安全保护条例（国令第745号）

[4] 信息安全等级保护管理办法（公通字［2007］43号））

[5] 关于加强工业控制系统信息安全管理的通知（工信部协［2011］451号）

[6] 工业控制系统信息安全防护指南（工信部信软［2016］338号）

1. 引用自GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南 4 定级原理及流程 [↑](#footnote-ref-1)