ICS 35.040
L 80



[illegible]

[illegible]

[illegible]

[

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义、缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 2
4　工业控制系统概述 …… 2
4.1　工业控制系统基本构成 …… 2
4.2　工业控制系统定级对象 …… 3
5　工业控制系统信息安全等级划分规则 …… 3
5.1　工业控制系统信息安全等级划分模型 …… 3
5.2　工业控制系统信息安全定级要素 …… 5
5.3　工业控制系统信息安全等级特征 …… 10
6　工业控制系统信息安全等级确定 …… 11
6.3　确定工业控制系统资产重要程度 …… 14
6.4　确定受侵害后的潜在影响程度 …… 14
6.5　确定需抵御的信息安全威胁程度 …… 20
6.6　确定工业控制系统信息安全等级 …… 22
附录 A（规范性附录）　有关生产安全事故和突发环境事件分级 …… 23
参考文献 …… 25

前　言

本标准按照GB/T 1.1给出的规

引　言

工业控制系统信息安全事关工业生产运行、国家经济安全和人民生命财产安全，为

本标准对工业控制系统信息安全等级保护作出规定，给出了基于

本标准第4章工业控制系统概述，描述了工业控制系统基本构成，工业控制系统定级对象；第5章工业控制系统信息安全等级特征；第6章工业控制系统信息安全定级方法，提出了工业控制系统信息安全定级流程；

工业控制系统信息安全分级规范

1 范围

本标准规定了基于风险评估的工业控制系统信息安全等级划分规则和定级方法，提出了等级划分
[illegible]等级的特征。
本标准适用于工业生产企业以及相
[illegible]部门和管理提供依据。

2 规范性引用文件

下列文件对于本文件的应
[illegible]是必不可少的。凡是注日期的引用文件，仅注日期的[illegible]版本适用于本文
件。凡是不注日期的引用文
[illegible]信息技术 安全技术 信息安全管理体系 要求 GB/T 22080—201[illegible]
GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
生产安全事故报告和调查处理条例 国务院第 493 号令
突发环境事件信息报告办法 环境保护部令第17号

3 术语和定义、缩略语

3.1 术语和定义

GB/T 22080—2016 界定的以及下列术语和定义适用于
3.1.1
信息安[illegible]

务规划和物流系统。对于其中第1层、第2层的相关系统、设备，可作为构成工业控制系统的范围。在实际工业生产系统实际环境中，可出现相邻两层的功能由一个系统、设备来实现，即在物理上并未分开，但并不影响所应实现信息安全控制措施的部署。

4.2 工业控制系统定级对象

对工业控制系统中相对独立的一部分，包括：

a) 单个的完整的工业控制系统：应以企业工业自动化生产过程为基础，属于企业的一个自动化生产全过程或一个工业自动化生产装置（如聚乙烯生产装置）的工业控制系统；

[illegible]全需求。

[illegible]，并选择其中最高的威胁程度。

[illegible]指在[illegible]

工业控制系统资产重要程度、受侵害后潜在影响程度、需抵御的信息安全威胁程度这三个

13。

度特征值，可在表1中查

资产重要程度特征值	受侵害后潜在影响程度特征值	需抵御的信息安全威胁程度特征值		
		1	2	3
1	1	第一级(1)	第一级(2)	第一级(3)
	2	第一级(2)	第一级(3)	第二级(4)
	3	第一级(3)	第二级(4)	第二级(5)
2	1	第一级(2)	第一级(3)	第二级(4)
	2	第一级(3)	第二级(4)	第二级(5)
	3	第二级(4)	第二级(5)	第二级(6)
3	1	第一级(3)	第二级(4)	第二级(5)
	2	第二级(4)	第二级(5)	第二级(6)
	3	第二级(5)	第二级(6)	第二级(7)
4	1	第二级(4)	第二级(5)	第二级(6)
	2	第二级(5)	第二级(6)	第二级(7)
	3	第二级(6)	第二级(7)	第三级(8)
5	1	第二级(5)	第二级(6)	第二级(7)
	2	第二级(6)	第二级(7)	第三级(8)
	3	第二级(7)	第三级(8)	第三级(9)

表 1（续）

资产重要程度特征值	受侵害后信息影响程度特征值	需抵御的信息安全威胁程度特征值				
		1	2	3	4	5
5	3	第二级(7)	第三级(8)	第三级(9)	第三级(10)	第四级(11)
1	4	第一级(4)	第二级(5)	第二级(6)	第二级(7)	第三级(8)
2	4	第二级(5)	第二级(6)	第二级(7)	第三级(8)	第三级(9)
3	4	第二级(6)	第二级(7)	第三级(8)	第三级(9)	第三级(10)
4	4	第二级(7)				
1	5	第二级(5)	第二级(6)	第二级(7)	第三级(8)	第三级(9)
2	5	第二级(6)	第二级(7)	第三级(8)	第三级(9)	第三级(10)
3	5	第二级(7)	第三级(8)	第三级(9)	第三级(10)	第四级(11)

5.2.1.2 工业控制系统行业领域

在工业控制系统资产重要程度要素构成中的工业控制系统行业领域是指，工业控制系统所在的工业生产行业领域，可分为关键领域、重点领域、一般领域，具体划分条件如下：

a) 关键领域的工业控制系统，是指属于国家关键基础设施的[illegible]工业控制系统，[illegible]关键基础设施是国家的重要战略资源；

b) 重点领域的工业控制系统，是指上述关键领域的工业控制系统以外，与国计民生紧密相关的工业生产领域中的工业控制系统，如[illegible]石化工[illegible]业、水利[illegible]

[illegible]

[illegible]况，可划分为资产作用价值很高、资产作用价值中等、资产作用价值一般，具体划分条件如下：

a) 资产作用价值很高的[illegible]控制系统应[illegible]符合下列条件之一：

1) 工业控制系统控制对象承担企业工业生产中的关键业务使命；

2) 当工业控制系统控制对象属于工业生产系统的核心生产部位，该控制对象[illegible]受到损害或丧失会[illegible]发生危险[illegible]无法[illegible]

[illegible]

[illegible]应符合下列条件之一：

工业控制系统控制对[illegible]企业工业生产中的一般业务使命；

当工[illegible]

[illegible]

[illegible]、资产获取价值一般，其

体划分条件如下：

a) 资产

5.2.2.2 受侵害的对象

在工业控制系统信息安全受侵害后潜在影响程度划分条件中的受侵害的对象是指工业控制系统

这些受侵害的对象可划分如下：

a) 工业

息安全威胁造成工业控制系统信息安全事件发生的可能性为

b) 当某个初始识别

家经济安全作为一个受侵害

工业控制系统需要抵御威胁的程度特征值取值范围从1～5，工业控制系统需要抵御威胁的程度特征值越高表示工业控制系统需要抵御威胁的程度越高。

5.2.3.2 面临的信息安全威胁

工业控制系统面临信息安全威胁主要从威胁来源、威胁表现形式和威胁程度等方面进行识别，并建立定级的工业控制系统的威胁列表。对工业控制系统面临信息安全威胁的识别，主要包括：

1) 威胁来源，是指威胁主体，可被描述为单个实体，也可以实体类或实体群体等方式来描述。威胁来源包括但不限于：

a) 人为因素，是指对工业控制系统资产的所有行为和其他技术因素，如在职员工误操作、硬件缺陷、软件开发缺陷、能源等公共服务供应失效等；

b) 故意的威胁：

2) 威胁表现形式，是指威胁来源对工业控制系统的威胁行为，如：

a) 信息攻击：可使工业控制系统的信息泄露或者提供有误的信息；

b) 通信攻击：可使工业控制系统的通信中断；

c) 对抗攻击：可使攻击者获得对工业控制系统的访问或使工业控制系统的数据

d) 非法使用：攻击者违反规定使用工业控制系统的资源，给工业控制系统运行带来长期的

e) 其他严重威胁：

或使得系统执

3) 威胁程度，是指来自有中等程度资源且愿意冒少量风险的威胁来源对于的攻击能力和有组织的四

对于拒绝服务攻击或者采用高级别复杂手段的威胁，以及发生在自然灾害等意外威胁下本标准推荐

[illegible]。

5.2.3.3 信息安全事件可能性

工业控制系统需抵御的信息安全威[illegible]

[illegible]度组合来评价。其中：

a) 根据 5.2.3.2 中的要求建立威胁列表，并对每个[illegible]分析其发生频率；

[illegible]定，得出工业控制系统信息安全事件可能性为“高”或“低”的结论。

5.3 工业控制系统信息安全等级特征

5.3.1 第一级工业控制系统

按照基于风险评估的信息安全等级划分的工业控制系统，第一级应[illegible]

a) 第一级工业控制系统信息安全受到破坏后，会对[illegible]的[illegible]

有以下主要特征：

[illegible]

[illegible]

[illegible]

面的安全防护保护

到所属企业依据国家有关管理规范和技术标准的保护[1]管

害；

够抵御来自敌对组织、有组织的团

外威胁，以及其他相当危

b) 第三级工业控制系统的信息安全保护，应使工业控制系统

体拥有中等程度资 故意威胁，严重的环境威胁，特别严重的意

安全事件影响的工业控制

措施，确保与组织的风险管理战略相

一致；连续监测系统日常和紧急事件，采取必要的应对措施，实施应急响应的执行和维护，防止事件扩大和减轻影响，采取改进措施，及时恢复受安全事件影响的工业控制系统运行等方面

维护国家安全的工业控制系统，以及需要抵御战争威胁或毁灭性自然灾难等意外威胁的工业控制系统，不在本标准的等级[2]中，可在管理和基础上另行制定增强控制措施

安全区域、通信网络；可按地理位置或管理责任划分，但应具有共同的安全需求；

3） 必要时，起传输作用的工业控制基础网络系统可作为单[illegible]定级对象。

c） 具有工业控制系统[illegible]

[illegible]

[illegible]

[illegible]责任；

2） 如果一个单位的甚至下级单位负责工业控制系统安全[illegible]

运维的第三[illegible]的全部安全

[illegible]

[illegible]

[illegible]

6.3 确定工业控制系统资产重要程度

6.3.1 评价工业控制系统安全领域和业务使命

评价作为定级对象的工业控制系统重要性相关内容，确认方法如下：

a) 按照 5.2.1.4 的[illegible]对工业控制系统资产进行分析，确定该工业控制系统的资产价值；

b) 根据工业控制系统所属工业生产行业分类进行分析，确定该工业控制系统的行业领域属于以下类型之一：

1) 一般行[illegible]

[illegible]业务使命。

6.3.2 评价工业控制系统资产重要程度

根据作为定级对象的工业控制系统行业领域、工业控制系统业务使命，按照 5.2.1.1 的要求，分析[illegible]工业控制[illegible]资产重要性相关内容，依照表 9 得出工业[illegible]等级；

6.4 确定受[illegible]在影响程度

6.4.1 确认工业控制[illegible]

统信息安全受到破坏

工业[illegible]

[illegible]

可靠性、可控性、业务连续性等：

完整的特性，确保工业控制系统能够以不受[illegible]预期的

系统故意的或意外的未授权操作，确保工业控制相关数

[illegible]

b) 完整性，是指保护工业控制[illegible]统资产准确和[illegible]

方式执行其预定功能，避免对工业控制

据没有遭受以未授权方式所作的更

到破坏的概况，并准确其中受到破坏最严重的

系统可控性、业务连续性）、系统

b） 对工业控制系统涉及的业务数据的破坏，是指工业控制系统中的相关数据、控制指令、保密信息等数据被窃取、篡改、伪造等，破坏工业控制系统业务数据的完整性、可用性、保密性。

由于工业控制系统服

的侵害程度的确认成为评

认，并选用受侵害后的潜在

顺序，逐一

统受到侵害，并由此产生对

患，造成危害国家的安全、

到侵害，并由此产生对

进行分析和选择：

a） 侵害国家安全的事项：

是指定级的工业控制系统信

受到侵害，及其造成工业生产系统

国家安全的影响，造成国家外部的威胁和侵害，造成内部的混乱和

荣誉和利益的行为，主要包括以下方面：

1） 影响国家政权稳固和国防实力；

2） 影响国家

5） 影响国家经济竞争力和科技实力；

6） 其他影

是指定级的工业控制系统信息安全

到侵害，及其造成工业生产

国家经济安全的影响，主要包括以下方面：

1） 影响国家

存在和发展所需资源有效供给；

2） 影响经济体系

独立稳定运行；

3） 影响整个

社会秩序稳定的影响，主要包括以下方面：

1）影响国家机关社会管理和公共服务的工作秩序；

2）影响各单位[illegible]经济活动秩序；

3）影响各行业的科研、生产秩序；

4）影响公众在法律约束下的正常生活秩序。

[illegible]是指定义[illegible]业控制系统信息安全事件被传播后，会造成工业生产系统受到侵害，并由此产生对公共利益及重要公共财产安全的影响，主要包括以下方面：

1）影响社会成员使用公共设施；

2）影响国有财产、劳动群众集体所有的财产安全或造成损失；

3）影响社会成员获取公开信息资源；

4）影响社会[illegible]

[illegible]行中断；

[illegible]影响工业生产运行安全并发生生产安全事故，甚至影响人员生命财产安全。

[illegible]失，并由此产生对其所控制的相关生产装置功能安[illegible]

3） 工业控制系统自身受到毁坏；

4）

或丧失；

6） 工业控制系统相关生产装置受到毁坏。

6.4.4 评价受侵害的

定对国家安全的侵害程度为

严重损害；

c） 特别严重损害：对国家的安全、荣誉和利益造成非常严重危害，可判定对国家安全的

度为特别严重损害

6.4.4.2 判定对国家

b) 严重损害：当对社会成员使用公共设施、获取公开信息资源、接受公共服务等公共利益产生较大范围的社会不良影响，对重要公共财产造成较高损失，可判定对公共利益、重要公共财产的侵害程度为严重损害；

c) 特别严重[illegible]会成员使用公共设施、获取公开信息资源、接受公共服务等公共利益产生大范围的社会不良影响，对重要公共财产造成极高损失，可判定对公共利益、重要公共财产的侵害程度为特别严重损害。

6.4.4.5 判定对环境安全和人员生命安全的侵害程度。

[illegible]的工作职能产生局部影响，业务能力有所降低但不影响主[illegible]

3） 可能出现严重的过程安全、业务连续性问题，或者较轻的人员安全、环境安全；

4） 对工业生产系统运行的地理区域、人群区域、生产生活领域、时间敏感影响方等；

5） 可能会发生一般、较大的生产安全事故或突发环境事件（见附录A）。

a） 一般损害：当对工业控制系统及相关装置产生局部影响或较轻影响，生产过程局部且非关键部位丧失完整性或可用性，轻微地干扰了生产过程的监视或操作员或协调性，未产生设备功能受到损坏，没有导致停工、重新加工、重新设计，对上游或下游生产过程没有产生影响，可判定对工业控制系统及相关装置的侵害程度为一般损害；

b） 严重损害：当对工业控制系统及相关装置产生严重影响，生产过程关键部位丧失完整性或可用性，不能在短时间内恢复工业过程控制，设备需要重新加工、重新设计，对上游或下游生产过程产生严重影响，或泄露敏感的知识产权丧失竞争优势（如生产过程的技术秘密），可判定对工业控制系统及相关装置的侵害程度为严重损害。

6.4.5 评价受侵害后的潜在影响

受侵害后潜在影响程度用关键指标表示，评价工业控制系统受侵害后

国家经济安全的侵害程度；选择其中侵害程度高的作为对“国家安全（特别是其中的国家经济安全）”的侵害程度；

2) 按照（[illegible]）4.3 [illegible]

[illegible]

[illegible]

[

附　录　A
（规范性附录）
有关生产安全事故和突发环境事件分级

重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）四级。为便于本标准应用，现将相关内容摘录如下。

A.2.2　突发环境事件分级条件摘要

A.2.2.1　特别重大（Ⅰ级）突发环境事件

凡符合下列情形之一的，为特别重大突发环境事件：

a）　因环境污染直接导致30人以上死亡或100人以上中毒的；

b）　因环境污染需疏散、转移群众5万人以上的；

c）　因环境污染造成直接经济损失1亿元以上的；

d）　因环境污染造成区域生态功能丧失或国家重点保护物种灭绝的；

e）　因环境污染造成地市级以上城市集中式饮用水水源地取水中断的；

f）　1、2类放射源失控造成大范围严重辐射污染后果的核设施发生需要进入场

中应急的严重核

事故，或事故辐射后果可能影响邻省和境外的，或按照“国际核事件分级（INES）标准[2]”属于3级以上的核事件；台湾核设施中发生的按照“国际核事件分级（INES

[redacted]

g) [redacted]应急状态标准的[redacted]，或进口货物严重辐射超标的事件；

h) 跨省（区、市）界突发环境事件。

[redacted]2.2.3 较大（Ⅲ级）突发环境事件

参 考 文 献

[1] GB 17859—1999 计算机信息系统安全保护等级划分准则

[2] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[3] GB/T 25069—2010 信息安全技术 术语