ICS 35.040
L 80

中华人民共和国国家标准

控制系统信息安全分级规范

Information security technology—
Information security classification specifications of industrial control systems

2018-06-07 发布　　　　2018-10-01 实施

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 …… [illegible]

　5.1　工业控制系统信息安全等级划分构成 …… [illegible]

　5.2　工业控制系统信息安全等级要素 …… [illegible]

　5.3　工业控制系统信息安全等级特征 …… [illegible]

[illegible]

　6.2　确定工业控制系统资产重要程度 …… [illegible]

　6.3　确定受到侵害后的影响程度 …… [illegible]

前　言

本标准按照 GB/T 1.1 [illegible] 给出的 [illegible]

[illegible] 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这 [illegible]

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，为了加强工业控制系统信息安全管理，对工业控制系统信息安全采取等级化管理。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，提出了等级划分模型和定级要素，包括工业控制系统资产重要程度、存在的潜在风险影响程度和需抵御的信息安全威胁程度，并提出了对工业控制系统信息安全划分四个等级。

[illegible]

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，提出了等级划分模型和定级要素，包括工业控制系统资产重要程 [illegible] 等级的特征。

本标准适用于工业生产企业以及相关行政管理部门，为工业控制系统信息安全等级的划分提供指导，为工业控制系统信息安全的规划、设计、运维以及评估和管理提供依据。

[illegible]

[illegible]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本文件。

3.1.1

信息安全 [illegible]

[illegible] 和/或资源的某些特性，这些特性用于定义安全 [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环境下，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。

d) 工业控制系统安全区域：对于比较大的或复杂的工业控制系统，对所有组成部分都采取同样等级的信息安全要求是不实际的或不必要的，需要将一个工业控制系统划分为若干个安全区域、通信网络。一个安全区域是采用共[illegible]需求的工业控制系统中的一组物理资[illegible]的一部分。一个安全区域应有一个边界，并于将包含的和被排斥的元素之间。一个通[illegible]安全区域之间连接的载体，具有共同[illegible]的安[illegible]

[illegible]

[illegible]工业控制系统在企业生产过程和业务体系的重要性，工业控制系统[illegible]关生产装置以及相关生产总值等资产综合价值；

b) 工业控制系统受侵害后潜在影响程度(5.2.2.1)，反映了工业控制系统[illegible]

[illegible]国家安全(特别是其中的国家经济安全)的影响；

[illegible]工业控制系统需抵御的信息安全威胁[illegible]

[illegible]可利用性、信息安全事件发生的可能[illegible]

[illegible]

准对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

[illegible]

等级特征值；

A ——表示工业控制系

统重要性；

N_A ——表示工业控制系

统重要程度的可接受特征值，以 [illegible]

制系统信息安全受侵害后潜在影响；

制系统信息安全受 [illegible]

[illegible] 威胁；

工业控制系统信息安全威胁程度的可接受特征值，以 [illegible] 的尺度来测量。

工业控制系统信息安全等级特征值 [illegible]

[illegible]

查出工业控制系统信息安全等级特征值，及其对应的工业控制系统信息安全

[illegible]

[illegible]	[illegible]	[illegible]	[illegible]	第二级(5)	第二级(6)	第二级(7)	[illegible]
[illegible]	[illegible]	[illegible]	4	3	第二级(5)	[illegible]	[illegible]

表 1（续）

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	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)	第三级(8)	第三级(9)	第三级(10)	第四级(11)
5	4	[illegible]	第三级(9)	第三级(10)	第四级(11)	第四级(12)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

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，如核设施、钢铁、有色、化工、石油石化、[illegible]力、天然气、先进制造、水利[illegible]境保护、铁路、城市轨道交通、民航、城[illegible]

[illegible]控制系统资产作用价值是指工业控制系统承担的业务使命、所处生产环节、受依赖程度等情[illegible]

[illegible]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[illegible]

[illegible]发生危[illegible]，而且无法[illegible]

[illegible]作用价值一般的工业控制系统应符合下列条件之一：

1) 工业控制系统控制对[illegible]企业工业生产中的一般业务使命；

2) 当工业控制系统控制对象属于工业生产系统的生产辅助部位，该控制对象功能受到损害[illegible]

[illegible]工业控制系统资产获取价值是指工业控制系统资产的原始成本[illegible]更换或再造成本，以及工业控制系[illegible]

统控制范围内相关工业生产装置设施价值……高、资产获取价值一般，其体划分条件如下：

a) 资产类

性的损失，导致生产过程丧失完整性或可用性，以及干扰了生产过程的正常运行或破坏而导致的物理资产的破坏而付出的成本一般

工业控制系统资产获取价值评价中"一般"、"很高"的具体数值，应依据工业生产各个行业的价值评价

系统出错等事件会对工业控制系统本身和其他相关受损害的对

造成的损害或后果，可能影响到一项或多项资产和

5.2.2.2 受侵害的对象

在工业控制系统[illegible]息安全受侵害后潜在影响程度划分条件中的受侵[illegible]信息安全受到破坏后，[illegible]不仅会对工业控制系统本身造成损失，还会对相关企业生产运行安全以及其他相关受侵害对象安全造成侵害。

[illegible]

[illegible]国家经济安全作为一个受侵害的对象，是强调工业控制系[illegible]

[illegible]

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[illegible]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[illegible]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[illegible]临信息安全威胁的识别，主要包括：

[illegible]威胁来源：是指威胁主体，可被描述为单个的实体，也可以实体类或实体联体等方式来描[illegible]

[illegible]可能意外地损害工业控制系统资产的所有行为和其他技术因素，[illegible]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；

2) 故意的[illegible]

[illegible]没有提供有价值的信息；

2) 通信攻击：可使工业[illegible]制系统的通信中断；

3) 网络攻击：可提供对工业控制系统[illegible]

[illegible]可采取病毒、蠕虫、自开发代码或木马等形式，给工业控制系统[illegible]行带来长期困扰，甚至严重损坏；

5) 特[illegible]

[illegible]破坏：破坏或使系统[illegible]理部件失效，如硬件、软件存储设备、接线、传感器和控制器；

[illegible]意外威胁，以及其他相当危害程度的威胁，其威胁程度[illegible]

[illegible]重的意外威胁，以及其他相当危害程度的威胁，其威胁程度特征

[illegible]重的环境威胁，特[illegible]

值为 4；

5) T5：是指来占有丰富[illegible]度资源的特别熟练对手的故意威胁（如敌对国家、敌对组织），特别严重的环境威胁，特[illegible]严重的意外威胁，以及其他相当危害程度的威胁，其威胁程度特征值为 5。

对于战争或威胁，包括来自国家级别敌方手段的威胁，以及突发性自然灾难等意外威胁，不在本标准考虑范围。

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胁 [illegible]

[illegible]

事件可能性；

e) 对威胁列表的每个威胁逐一给出信息安全事件发生的可能性“高”或“低”，[illegible]

[illegible]

[illegible] 和其他组织的合法权益及重要财产造成损 [illegible] 家经济安全、环境安全、社会秩序、公共利益和人员生命；

b) 第一级工业控制系统的信息安全保护，应使工业控制系统能够抵御来自个人、拥有少量资源的 [illegible]

[illegible]

[illegible] 工业生产运行造成重大损害，或者对重点领域的工业生产运行造成损害，或者对公民、企业和其他组织的合法权益及重要财产造成严重损害，或者对环境安全、社会秩序、公共利益和人员生命造成损害，但不会损害国家安全（特别是其中的国家经济安全）；

b) 第二级工业控制系统的信息安全保护，应使工业控制系统能够抵御来自有组织的团体、拥有中 [illegible]

面的安全保护[illegible]

c) 第[illegible]级工业控制系统[illegible]息安全应得到

所属企业依据国家有关管理规范和技术标准的保护[illegible]管

[illegible]损害；

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

能够抵御来自敌对组织、有组织的团

体拥有中等程度资[illegible]的故意威胁、严重的环境威胁、特别严重的意

外威胁，以及其他相当危[illegible]

[illegible]受安全事件影响的工业控[illegible]

[illegible]安全保护能力；

a) 第四级工业控制系[illegible]

信息安全受到破坏后，会对关键领域的工业生产运行造成重大损害，或者

对环境安全、社会秩[illegible]

家、公共利益和人员生命造成特别严重损害，或者对国家安全（特别是其中

的国家经济安[illegible]

造成严重损害；

b) 第四级工业控[illegible]

系统的信息安全保护，应使工业控制系统能够抵御来自敌对组织、拥有丰富资

源的故意威胁[illegible]

c) 第四[illegible]

管理[illegible]

略，实施信息安全治理；采取较全面的信息安[illegible]

止事件扩大和减轻影响，采取改进措施，对[illegible]受安全事件影响的工业控制系统进行等方面

的安全保护[illegible]能力；

d) 第四级工业控制系统信息安全应得到所属企业依据国家有关管理规范和技术标准的管理，以

及国家主管部门和信息安全监管部门强化的监督、检查。

另外，对于直[illegible]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[illegible]

业控制系统信息安全定级流程是一致的，定级流

位或下位关系或少量控制

装置中一个相对独立的区域，与其他业务应用的控制过程有

信息交换，可能会

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 级对象。

c） 具有工业控制系统

有安全

控制系统的基本信息

1） 工业控制系统与其归属的工业生产装置的目的、任务和使命；

2） 工业控制系统的控

业控制系统对可用性

和保密性等方面的重要性。

e） 工业控制系统 相关协议，以及这些数据在保密性、完整性和可用性等方面的重要性。

f） 工业控制系统与企业相关信息系统的连接，包括连接方式、接口控制、传输

相关用户营

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[illegible]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[illegible]

[illegible]潜在影响

程度

安全受到破坏

6.4.1 确认工业控制系统信息

工业[illegible]

[illegible]控制系统

[illegible]可靠地运行，防止正常服务的终止[illegible]

响应性，如要求系统响应时间可在毫秒级以内；可靠性

可控性、业务连续性等；

b) 完整性：是指保护工业控制系统资产准确和完整的[illegible]

[illegible]性，确保工业控制系统能够以不受[illegible]的

方式执行其预定功能，避免对工业控制[illegible]系统[illegible]

意的或意外的未授权操作，确保工业控制相关数

据没有遭受以未授权方式所作的更改或破坏

[illegible]

人、实体、进程，或不被其利用的特性，通[illegible]

到破坏的情况，并选择其中受到破坏最严重[illegible]

[illegible]破坏工业控制系统的可用性（如系统可控性、业务连续性）、系统[illegible]性、保密性；

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、泄露等，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[illegible]

[illegible]分别处理这两种危害[illegible]受侵害对象的侵害程度的确认应按照工业控制系统服务安全和工业控制系统业务数据安全方式分别进行分析确认，并选用受侵害后的潜在[illegible]

[illegible]顺序，逐一

产系统受到侵害，并由此产生对

和疾患，造成危害国家的安全、

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[illegible]受到侵害，及其造成工业生[illegible]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[illegible]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) 影响国家统一、民族团结和社会安定；
3) 影响国家对外活动中的政治、经济利益；
4) 影响国家重要的安全保卫工作；
5) 影响国家经济竞争力和科技实力；
6) 其他影响[illegible]

[illegible]

是指定级的工业控制系统信息安[illegible]经济安全的影响，主要包括以下方面：

1) 影响国家[illegible]存在发展所需资源的有效供给；
2) 影响经济体系独立稳定运行；
3) 影响整体[illegible]

[illegible]级工业生产系统[illegible]受到侵害，并由此产生对

工业控制系统及工业生产系统的[illegible]条件环境、相关自然生态环境，造成[illegible]

[illegible]造成集中式饮用水水源地取水中断，造成[illegible]

严重辐射污染环境等。

d) 侵害公民、企业和其他组织的合法权益及重要财产安全的事项：

是指定级的工业控制系统信息安全[illegible]对公民、企业和其他组织[illegible]权益及财产安全的影响，主要包括以下方面：

1) 影响由法律确认的并受法律保护的公民、企业和其他组织所享有的社会

权利和利益；

2) 影响公民、企业和其他组织所有的资金和物质财产损失[illegible]

[illegible]正常；

[illegible]全丧失；

2) 工业控制系统自身功能完

3） 工业控制系统自身受到毁坏；

常；

5） 工业控制系统相关生产装置功能受

损害或丧失；

国家安全的侵害程度为

严重损害；

c） 特别严重损害

限的社

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[illegible]不良影响，对重要公共财产造成较高[illegible]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[illegible]

[illegible]下列等级之一：

1) 特别重大(Ⅰ级)突发环境事件；
2) 重大(Ⅱ级)突发环境事件；
3) 较大(Ⅲ级)突发环境事件；
4) 一般(Ⅳ级)突发环境事件。

6.4.4.6 判定对公民、企业和[illegible]织的合法权[illegible]及重要财产安全的侵害程度

当工业控制系统信息安全受到破坏时，造成对公民、企业、其他组织的合法权益及重要财产安全的侵害程[illegible]

[illegible]

[illegible]组织的合法权益及[illegible]财产[illegible]的侵害程度为严重损害；

c) 特别严[illegible]

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[illegible]区域、人[illegible]域、生产生活领域、时间[illegible]影响较小；

5) 不会发生生产安全[illegible]

[illegible]能立即通过程序予以修复；

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、时间跨度影响为中等；

5) 可能会发生一般(较大)生产安全事故或突发环境事件(见附录 A)。

c) 特别严重损害：判定对工业生产系统运行安全的侵害程度为[illegible]

[illegible].4.8 判定对工业控制系统及相关生[illegible]害程度

当工业控制系统信息安全受到破坏时，造成对工业控制系统及相关装置的侵害程度，判定条件如下：

a) [illegible]

[illegible]的侵害程度为一般损害；

b) 严重损害：当[illegible]工业控制系统及相关装置产生关键部位的影响或严重影响，生产过程关键部位丧失完整性或可用性，严重地干扰了生产过程的准确顺序或协调性，产生[illegible]设备功能受到损害[illegible]或[illegible]关但[illegible]本不高，导致短时间的停工且在短时间内恢复工业过程控制，对上游或下游生产过程产生较[illegible]影响，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；

c) 特别严重损害：当对工业控制系统及相关装置产生全[illegible]影响或特别严重影响，生产过程全[illegible]

[illegible] 评价受侵害后的潜在影响程度

受侵害后潜在影响程度用其特征值表示，评价工业控制系统受侵害[illegible]

[illegible]

国家经济安全的侵害程度，选择其中侵害程度高的作为对

[illegible]威胁列表；

2）查阅企业、行业或业界已有的威胁列表和统计数据；

3）查阅国际组织发布的关于定级的工业控制系统及其组件面临的威胁；

4）收集定级的工业控制系统及其组件以往安全事件报告中出现过的威胁；

5）收集定级的工业控制系统有关现场检测工具以及各种[illegible]日志及现场控制威胁；

汇集上述威胁信息被综合分析，建立定级的工业控制系统可能面临威胁的列表。

b）根据5.2.3.2c)，对上述威胁列表中每个威胁评价其威胁程度并[illegible]

b） 比较定级的工业控制系统需抵御的所有信息安全威胁，选择其中威胁程度特征值（取值范围为

1～5）最高者，判定

根据 6.1 的要求，用已确定的工

业控制系统资产重要程度特征值、受侵害潜在影响程度特征值

抵御的信息安全威胁 特征值，在表

1 中查找对应等级别，即可 于工业控制系统信息安全风险

的工业控制系统信息安全等级。

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

[illegible] 亿元以上直接经济损失的事故；

（二）重大事故，是指造成10人以上30人以下死亡，或 [illegible]

[illegible] 中，规定了突发环境事件分级的标准，[illegible] 突发环境事件严重性和紧急程度，突发环境事件 [illegible] 大（Ⅰ级）、重大（Ⅱ级）[illegible]

[illegible] 亡或 100 人以上中毒的；

b） 因环境污染需疏散、转移群众 5 [illegible] 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 [illegible]

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

[illegible]

区或居民聚集区、医院、学校等敏感区域的；

g) 1、2类放射源丢失、被盗、失控造成环境影响，或核设施和铀矿冶炼设施发生的[illegible]入场区应急状态标准的[illegible]，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。

2.2.3 较大(Ⅲ级)突发环境事件

[illegible]

---

2) “国际核事件分级(INES)标准”是由国际原子能机构(IAEA)[illegible]经济合作与发展组织核能机构(OECE/NEA)于1990年共同制订的有关核事件分级文件，国际上通常采用国际核事件分级(INES)标准对核电厂事件进行分级。[illegible]国防科工委于2001年发布的《国际核事件分级和事件报告系统管理办法(试行)》，也使用了国际核事件分[illegible]

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

[4] GB/T 29246—201[illegible] 信息技术 安全技术 信息[illegible]

[illegible] 关于加强工业控制系[illegible]