ICS 35.040
L 80

工业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　　2019-01-01 实施

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1

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

工业控制系统信息安全分级规范

1 范围

本标准规定了[illegible]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]

[illegible]等级的特征。

[illegible]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[illegible]

[illegible]设计、运维以及评估和管理提供依据。

本标准适用于工业生产企业以及相[illegible]

导，为工业控制系统信息安全的规划、[illegible]

[illegible]sk

特定威胁利用单个或一组资产脆弱性的可能[illegible]

性以及由此可能给组织带来的损害。

注：它以事态的可能性及其[illegible]

务规划和物流系统。对于其中第3层、第2层的相关系统、设备，可作为构成工业控制系统的
节点。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。

b) 工业控制系统安全区域：对于比较大的复杂的工业控制系统，对所有组成部分都采取同样等
级的安全措施是不实际的或不必要的，需要将一个工业控制系统划分为一个个安全区域、通信网
络。一个安全区域是采用共同[illegible]安全需求的工业控制系统中的一组物理资[illegible]
[illegible]的一部分。一个安全区域应有一个边界，介
于被包含的和被排斥的元素之间。一个[illegible]安全区域之间连接的载体，具有共同
的安

对独立的一部分实施[illegible]

可对一个具体的完整的工业控[illegible]

统中相对独立的一部分的信息安全

[illegible]

[illegible]

[illegible]

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

等级。

表 1

工业控制系统信息安全防护等级对照表

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[illegible]工业控制系[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[illegible]

[illegible]程度可[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[illegible]：

a) 资产作用价值很高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[illegible]受到损害或丧失会[illegible]

[illegible]发生危险[illegible]属于工操作使[illegible]系统的告[illegible]值很高。

[illegible]

工业生产系统正常运行；

4)，工业控制系统所属的工业生[illegible]

b) 资产作用价值中等的工业控制系[illegible]

统控制范围内相关工业生产装置设施价值一般，其

体划分条件如下：

a) 资产类

一般；

或者其抽象价值一般；

2) 工业控制系统设备本身更换或再造成本一般，或者因

和保密

5.2.2.1 受侵害后潜在影响程度

受侵害后潜在影响程度是工业控制系统信息安全等级的定级要素之一，由受侵害的对象(5.2.2.2)和受侵害的程度(5.2.2.3)两个

工业控制系统受侵害后潜在影响程度特征值越高表示工业控制系统受侵害后潜在影响程度越

5.2.2.2 受侵害的对象

在工业控制系统[illegible]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[illegible]受侵害的对象可划分如下：

a) [illegible]

b) [illegible]

c) 社会秩序、公共利益、环境安全和人员生命安全；

d) 国家安全(特别是其中的国家经济安全)。

5.2.2.3 受侵害的程度

工业控制系统信息安全受到侵害是指工业控制系统的可用性[illegible]

[illegible]最高的作为选择依据。

在工业控制系统受侵害后潜在影响程度划分条件中的受侵害的程度是[illegible]工业控制系统信息安全受到破坏后[illegible]

的信息安全威胁(5.2.3.2)和信息安全事件可能性(5.2.3.3)确定。

根据信息安全事件发生的可能性水平对初始已识别的工业控制系统面临所有信息安全威胁(即威胁列表)进行取舍，包括：

a) 当某个初始识别的信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“高”时，则该信息安全威胁应保留，即确认为需要抵御的威胁；

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，是指威胁主体可以类似或修改单个或实体，也可以实体类或实体群体等方式来描

[illegible]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，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；

2) 故意的[illegible]

[illegible]

3) [illegible]因造工业控制系[illegible]的数据；

4) 恶意代码[illegible]可采取病毒、蠕虫、自开发代码或木马等形式

[illegible]破坏：破坏或使系统物

部件失效(如硬件、软件存储设备、接线、传感器和控制器)，

[illegible]或便得系统执[illegible]

[illegible]获得很大风险的对手的[illegible]故意威胁(如个人、有组织的较小[illegible]团体

，一般的环境威胁，严重的意外威胁，以及其他相当危害程度的威胁。其威胁程度值

对于战争威胁、恐怖袭击国家级别重大事故的威胁，以及发生在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

d) 根据固有脆弱性可利用容易度和威胁发生的频度，对威胁列表中每个威胁逐一分析信息安全事件可能性；

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]

面的安全防护能力。

b) 第三级工业控制系统的信息安全保护，应使工业控制系

体抱有中等程度资

成资产损

c) 第四级工业

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独的定级对象。

c） 具有工业控制系统

生产装置

提供整合

的系统可用多个厂家的设备与系统组成，所有功能协调一起为工业

3） 避免将

个单一的系统组件，如服务器、控制终端、网络设备、通信路

b） 比较

功能用、风险状况。

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[redacted]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[redacted]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[redacted]

[redacted]

[redacted]高[redacted]3个等级。

6.4 确定受[redacted]安全[redacted]潜在影响程度

6.4.1 确认工业控制系统信息安全受到破坏

工业[redacted]

到破坏的情况，并选择其中受到破坏最严重的安全属性的破坏程度，作为工业控制系统信息安全受到破坏的程度。

6.4.2 依据侵害的客观方面进行分析

[illegible]

[illegible]

[illegible]

环境安全的影响，主要包括以下方面：

1） 工业控制系统及工业生产系统的生[illegible]类性环境、相关自然生态环境，造成污[illegible]破坏；

2） 因环境污染[illegible]直接导致人员死亡或中毒、造成人员疏散转移、造成直接经济损失、造成区域生态功能丧失或国家重点保护物种灭[illegible]、造成集中式饮用水水源地取水中断、造严重辐射污染后果等。

b） 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]到侵害，及其造成工业生产系统受到侵害，并由此产生对

[illegible]相关人员的伤害。

3） 影响工业生产系统运行安全，引发的工业生产安全事故；

4） 影响公民、企业和其他组织的人员生命安全，直接或间接造成

c） 侵害工业生产运行安全的[illegible]事项：

是指定级的工业控制系统信息安全[illegible]到侵害，并由此产

失，并由此产生对其所控制的[illegible]

3） 工业控制系统自身受到毁坏；

常；

损害或丧失；

6.4.4 评价受侵害的

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侵害程度为特别严重损害。

6.4.4.2 判定对国家经济安全的侵害程度

工业控制系统信息安全受到破坏时，造成对国家经济安全的

不良影响，对重要公共财产造成较小损失，可判定对公共利益、重要公共财产的侵害程度为一般损害；

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]较大(Ⅱ级)突发环境事件；

3) 较大(Ⅱ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[illegible]

[illegible]、企业、其他组织的合法权益及重要财产安全的侵害程度为严重损害：

c) 特别严[illegible]

[illegible]

[illegible]

国家级涉密会的信息程度，选择其中信息程度高的作为对

系统发生变化时，评价信息安

中威胁源发生的频度；

件报告中各种日志中或现场测试工具发现的威胁

制系统的信息资产发生的频度；

控制系统的威胁发生的频度；

可能性包括：

a) 根据 6.5.1 形成的威胁列表，对确定存在每一

1) 收集定级的工业控制系统以往安全

发生的频度；

2) 收集行业（或企业）内类似工业控

3) 收集国际组织发布的类似工

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

国务院安全生产监督管理部门和设区的市级以上人民政府负责安全生产监督管理的部门会同国务院有关部门，制定事故等级划分的补充性规定。

本条款所称的“以上”包括本数，所称的“以下”不包括本数。

A.2　突发环境事件分级

[illegible]中，规定了突发环境事件分级[illegible]的标准，[illegible]突发环境事件严重性和紧急程度，突发环境[illegible]事件[illegible]分为特大[illegible]级、重大[illegible]级、较大[illegible]级

[illegible]亡或100人以上中毒的；

b）　因环境污染需[illegible]

[illegible]

[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

c) 一次性造成直接经济损失500万元以上2 000万元以下的；

d) 因环

除特别重大突发环境事件、重大突发环境事件、较大突发环境事件以外的突发环境事件。

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

[4] GB/T 29246—2017