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

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 …… 4

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[illegible]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[illegible]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的特征。

本标准[illegible]工业控制系统信息安全等级划分规则[illegible]工业控制系统信息安全等级划分模型，工业控制系统信息安全定级[illegible]素，工业控制系统[illegible]

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[illegible]

[illegible]等级的特征[illegible]

[illegible]本标准适用于工业生产企业以及相[illegible]

[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]导，为工业控制系统信息安全的规划、[illegible]

设计、运维以及评估和管理提供依据。

[illegible]

[illegible]

[illegible]

务规划和物流系统。对于其中第 1 层～第 3 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中

a) 一个具体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；

b)

对工业控制系统中相对独立的一部分定级的建议与指导，信息安全防护设计的需要，根据具体需要对一个具体的完整的工业控制系统或其中相对独立的一部分分别定级。一般情况下工业控制系统中相对独立的一部分的信息安全等级不应高于其整体的工业控制系统的信息安全等级。

5 工业控制系统信息安全等级划分规则

5.1 工业控制系统信息安全等级划分类型

本标准规定的工业控制系统信息安全等级是基于工业控制系统资产重要程度、威胁和脆弱性，以及威胁发生后对工业生产业务的影响程度，在工业控制系统普遍存在的威胁中，依据工业控制系统和其中相对独立的一部分的特性，以及工业控制系统资产、威胁、脆弱性、安全事件发生后对工业生产业务潜在影响程度的考虑，

和工业控制系统信息安
级要求的姓征值

表1 工业控制系统信息安 全等级对

需抵御的信息安全威胁程度特征值				
	2	3	4	5
级(1)	第一	第一级(3)	第一级(4)	第二级(5)
	第一级(2)	第一级(3)	第一级(4)	第二级(5)

资产重要程度特征值	受侵害后潜在影响程度特征值	
1	1	第一
2	1	

				第二级(5)	第二级(6)
9)	第三级(10)		4	3	第二级(6)

第二级(6)	第二级(7)	第三级(8)
4		

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)				
						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工业控制系统，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，如石油石化、电力、天然气、供水供热、制造、水利[illegible]、环境保护、铁路、城市轨道交通、民航、城[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[illegible]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]主要生产流程产生中断或对主要生产流程产生严重影响；

3) 工业生产系统对该工业控制系统的依赖程度高，当该工业控制系统[illegible]手工操作使工业生产系统正常运行；

4) 工业控制系统所属的工业生产系统的生产连续的生产[illegible]很高。

b) 资产作用价值中等的工业控制系统[illegible]

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，工业控制系统信息安全受到破坏后，不同人群对工业控制系[illegible]

[illegible]受侵害的对象可划分如下：

a) [illegible]

[illegible]

d) 国家安全(特别是其中的国家经济安全[illegible])。

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[illegible]

[illegible]

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

[illegible]

[illegible]则

[illegible]

该信息安全威胁应保留，即确认为需要抵御的威胁。

[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：

a) 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群体等方式来描述，包括：

1) 意外的威胁，是指非恶意人员[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，如合法的职员工误操作、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]灾为行为的损害工业控制系统资产的所有事件，如地震、洪水、风暴等自然灾害。

b) 威胁表现形式，是指威胁主体对资产执行的动作，这些动作会影响资产的[illegible]

[illegible]入侵者提供有价值的信息；

2) 通信攻击：可使工业[illegible]产制系统的通信中断；

[illegible]其生产受损坏；

[illegible]资源且总是[illegible]少量风险的对手的敌意威胁（如个人），一般的环境[illegible]威胁，一般偷窃威胁，以及其他相当危害程度的威胁，其威胁程度特征值为1；

2) [illegible]

2：是指来自占有少量资源[illegible]

对于拒绝服务、违背来自高级别未授权的威胁，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

工业控制系统零抵御的信息安全威胁

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”

相当危害程度威胁所造成资产损失的

信息安全风险

第一级工业控制系统应至少具有对系统资产、运行环境、安全风险的基本认识，采取基本的信息安全控制措施，检测系统异常和安全事件，应急响应的执行和维护，防止事件扩大和减轻影响，基本恢复受安全事件

d） 第一级工业控制系统信息安全应得到所属企业依据国家有

管理

5.3.2 第二级工业控制系统

按照基于风险评估的信息安全等级划分的工业控制系统

c） 第二级工业控制系统应至少具有对系统资产、运行环境、安全风险的比较全面认识，初步建立风险管理战略；采取比较全面的信息安全控制措施；及时检测系统异常和安全事件；应急响应的执行和维护；防止事件扩大和减轻影响；基本恢复受安全事件

工业控制系统运行

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

害；

能够抵御来自敌对组织、有组织的团

外威胁，以及其他相当危害

b） 第三级工业控制系统的信息安全保护，应使工业控制系

体和有中等程度资源动机故意威胁，严重的环境威胁，特别严重的

，行和维护，防止事件扩大和减轻影响；恢

复受安全事件影响的工业控制

国家主管部门

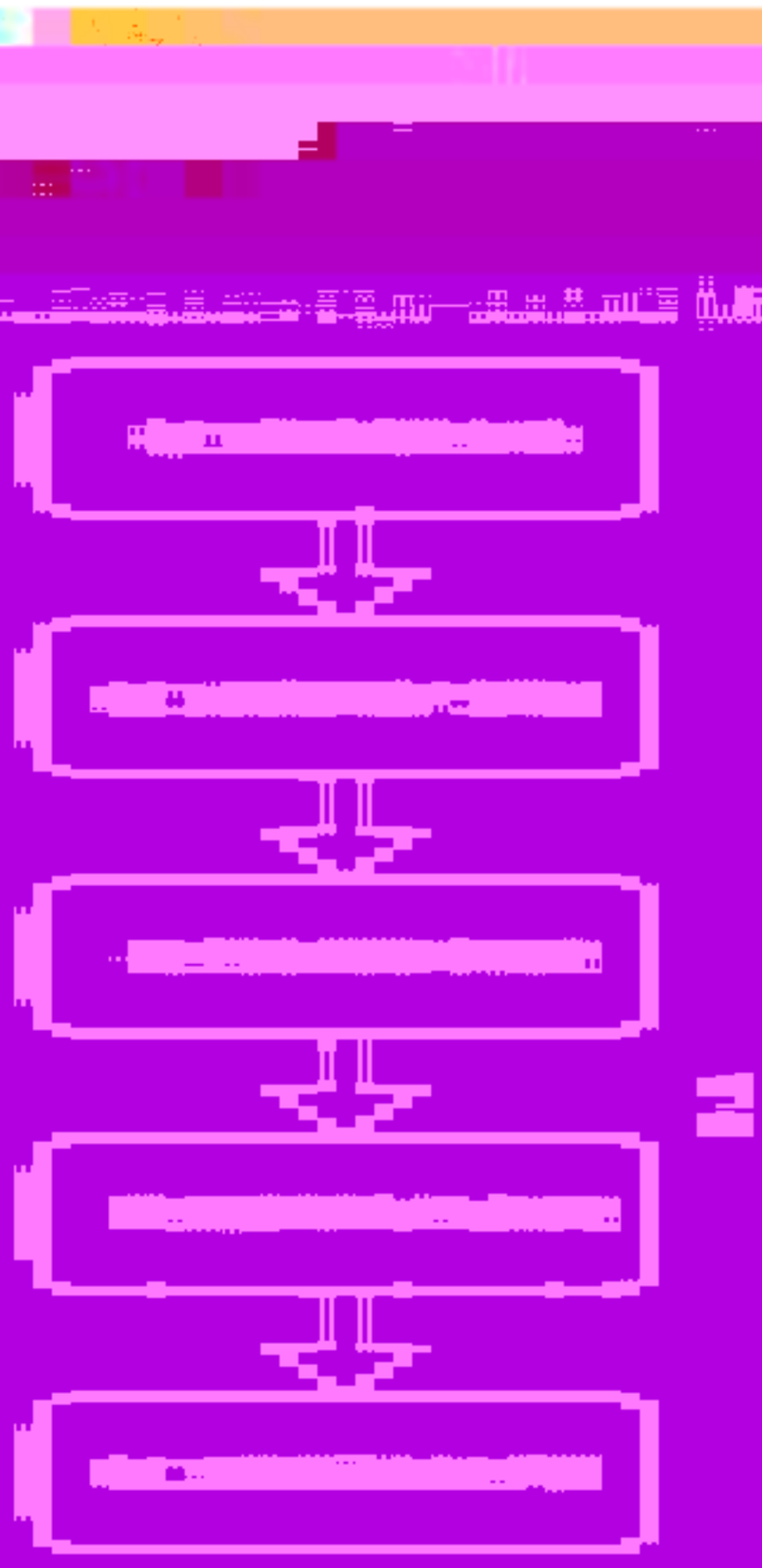
信息安全监管部门的监督、检查。

5.3

[illegible]

[illegible]

[illegible]



其他业务应用的控制过程没有产生

站、操作员工作站、数据采集接口或控制接口，以及相关网络等其他设施组

b） 工业控制系统中相对独立的一部分：

1） 承载“相对独立”的工业控制过程中一部分业务（应用或控制过程独立，如

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]级对象。

c） 具有工业控制系统[illegible]

[illegible]控制过程；

2） 一个工业控制[illegible]

[illegible]

[illegible]确定的安全[illegible]

[illegible]

对象的工业控制系统应[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

对作为定级对象的工业控制系统描述应包括

a） [illegible]

[illegible]

[illegible]

[illegible]务过程及其相关连的列表；

b） 工业控制系统的网络设备、[illegible]

[illegible]

[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[redacted]家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]在影响程度

统信息安全受到破坏

6.4.1 确认工业控制系

工业[redacted]

[redacted]

[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

在客观方面，对受侵害对象的侵害外在表现为对工业控制系统[illegible]工业控制系统的危

[illegible]

[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、伪造，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务[illegible]全和工业控制系统业务数据”

[illegible]认，并选用受侵害后的[illegible]

[illegible]序，逐一

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，及其造成工业生产系统受到侵害，并由此产生对国家安全的影响，造成国家外部的威胁和侵害，造成内部的混乱和疾患，造成危害国家的安全、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]到侵害，并由此产生对

是指定级的工业控制系统信息安全[illegible]受到侵害，及其造成工业生产系统受到侵害，并由此产生对国家经济安全的影响，主要包括以下方面：

1) 影响国家[illegible]持其经济存在和发展所需资源有效供给；

2) 影响经济体系[illegible]独立稳定运行；

3) 影响整个社会[illegible]

3） 工业控制系统自身受到毁坏；

4）

正常；

5） 工业控制系统相关生产装置功能受

到损害或丧失；

判定对国家安全的侵害程度为

严重损害；

c） 特别严重损害：

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[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]

[illegible]Ⅱ级)突发环境事件：

[illegible]一般Ⅱ级突发环境事件。

6.4.4.6 判定对公民、企业和[illegible]其他组织的合法权[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度[illegible]

[illegible]

[illegible]

[illegible]

[illegible]业生产系统运行安全的侵害程度为一般损害的条件为：

1) 对工业生产系统的任务无影响、整体功能有所下降或一部分任务不能完成；

2) 出现[illegible]分系统故障或功能下降，能够通过调整消除故障或能够[illegible]修复出现的故障；

[illegible]能出现较好的过程安全、业务连续性[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、时间敏感影响为[illegible]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]害程度

[illegible]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

[illegible]4.8 判定对工业控制系统[illegible]发生[illegible]

当工业控制系统信息安全受[illegible]如下：

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]

定对公共利益及重要公共财产安全的侵害程度；按照 6.4.4.5 提供的方法，判定[illegible]全和人员生命安全的侵害程度；选择其中侵害程度最高的作为对“环境安全、社会秩序、公

[illegible]的对受侵害对象的侵害程度按照下列受[illegible]程度之一[illegible]

[illegible]个受侵害对象，以及根据 b）判定的[illegible]

[illegible]按照 5.2.2.1[illegible]

[illegible]要求，[illegible]业控制系统受侵害后潜在影响的相关内容，分别依照表 3 得出[illegible]工业控制系[illegible]

[illegible]统受侵害潜在影响程度特征值，并选[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

威胁

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）最高者判定为定级的工业控制系统需抵御的信息安全威胁程度特征值。

6.6 确定工业控制系统信息安全等级

1 的要求，由已确定的

工业控制系统资产重要程度特征值、受侵害类别及影响程度特

抵御的信息安全威胁

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]

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[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]

[illegible]亡或100人以上中毒的；

b）　因环境污染[illegible]

流散、转移群众[illegible]人以上的；

c）　因环境污染[illegible]

造成直接经济损失1亿元以上的；

d）　因环境污染[illegible]

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[illegible]

造成地市级以上城市集中式饮用水水源[illegible]取水中断的；

f）　1、2类放[illegible]

[illegible]源突发性造成大范围严重辐射污染后果的核设施发生需要场外应急的严重核

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

凡符合下列情形之一的，为较大突发环境事件：

a） 因环境污染直接导致3人以下死亡或10人以上50人以下中毒的；

b） 因环境污染需疏散、转移群众5 000人以上1万人以下的；

c） 因环境污染造成直接经济损失500万元以上2 000万元以下的；

d） 因环境污染造成国家重点保护的动植物物种受到破坏的；

e） 因环境污染造成乡

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