ICS 35.040
L 80

工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-

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 …… 4
5.1　工业控制系统信息安全等级划分概述 …… 4
5.2　工业控制系统信息安全等级保护 …… 4
5.3　工业控制系统信息安全等级特征 …… 4
5.4　确定工业控制系统资产重要程度 …… 5
5.5　确定受到破坏后的安全影响程度 …… 5

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的

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。

本标准适用于工业生产企业以及[illegible]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。

2 规范性引用文件

[illegible]

3 术语、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

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

一般情况下，工业生产系统中，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。

b) 工业控制系统安全区域：对于结构关系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或多个安全区域、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]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除的元素之间。一个[illegible]络是连接两个安全区域之间连接的载体，具有共同[illegible]的[illegible]

关生产总值等资产

综合价值；

b) 工业控制系统受[illegible]

事后潜在影响程度(5.2.2.1)，反映了工业控制系统[illegible]

国家安全(特别是其中的国家经济安全)的影响；

[illegible]系统需抵御的信息安全威胁[illegible]

[illegible]利用性、信息安全事件发生的可能

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

统重要性；

统重要程度的可接受特征值，以

制系统信息安全受侵害后潜在影响；

制系统信息安全受

A ——表示工业控制系

N_A ——表示工业控制系

表示工业控

表示工业控

表

区

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

					第二级(5)	第二级(6)	第
			4	3	第二级(6)		

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

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[指对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[如石化、化工、石油石化[境保护、铁路、城市轨道交通、民航、城

[工业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[受攻击[

对象层工业生产系统节点[心生产部位，该控制

发生危[险，而且无法

c) 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[象为]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节点

[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]更换或再造成本，以及工业控制系

统控制范围内相关工业生产装置设备的价值

体划分条件如下：

a) 资产类

性的损失，导致生产过程无法完全正确可用性，以及不执行工业控制的策略或可能
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

统本身和其他相关受侵害的对

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]信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，不仅会对工业控制系统本身造成损失，还会对相关工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]

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。对工业控制系统所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，可被描述为单个的实体，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) 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，如合法但职员工误操作、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

c) 提供有价值的信息；

d) 通信攻击：可使工业控制系统的通信中断；

e) 恶意网络攻击：可提供对工业控制系统

f) 恶意软件：可采取病毒、蠕虫、自开发代码或木马等形式，给工业控制系统运行带来长期困扰，甚至严重损坏；

g) 特定级别

h) 物理破坏：破坏或包括但不限于硬件失效、如硬件、软件存储设备、接线、传感器和控制器；

i) 环境威胁，以及其他相当危害程度的威胁，其威胁程度特征值为4；

j) T5：是指来占有丰富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，以及其他相当危害程度的威胁，其威胁程度特征值为5。

对于拥有少量资源的

考虑的威胁范围。

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

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”；

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

对重点领域的工业生产运行造成重大损害，或者

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）；

面的安全生产能力。

所属企业依据国家有关管理规范和技术标准的保护管

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

体拥有中等程度资源的故意威胁，严重的环境威胁，特别严重的意

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

序、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

造成严重损害；

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

对环境安全、社会秩

的国家经济

b） 第四级工业控

源的故意威胁

管理

的安全保护

的安全保护能力；

d） 第四级工业控制系统信息安全保护应使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，对于直接

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

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一级对象。

c） 具有工业控制系统

业生产装置的目的、任务和使命；

这些数据在保

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[redacted]

程度

安全受到破坏

6.4.1 确认工业控制系统信息

工业[redacted]

[redacted]

[redacted]

到破坏的概因，并准确其中受到破坏导致[illegible]

系统可控性、业务连续性）、系统[illegible]生、保密性：

b） 对工业控制系统涉及的业务数据的破坏，是把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、损毁等，破坏工业控制系统业务数据的完整性、[illegible]性、保密性，由于工业控制系统服[illegible]

[illegible]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[illegible]力；

6） 其他影响[illegible]

7） 影响经济体系总体稳定运行；

8） 影响整个[illegible]

9） [illegible]工业生产系统受到侵害，并由此产生对

[redacted]

[redacted]

[redacted]

3） 工业控制系统自身受到毁坏；

4）

常；

5） 工业控制系统相关生产装置功能受

损害或丧失；

c） 特别严重损害：

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]突发环境事件等级根据下列[illegible]等级之一：

1) 特别重大(Ⅰ级)突发环境事件；

2) 重[illegible]大(Ⅱ级)突发环境事件；

3) [illegible]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[illegible]侵害[illegible]

[illegible]

[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、时间敏感影响较小；

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

害程度

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

一般损害；

产生关键部位的影响或严重影响，生产过程关键部位

过程的准确顺序或协调性，产生

本不高导致短时间的停工且在短时间内恢复工业控制；对上

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；

制系统及相关装置产生全

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后

国家级涉密企业的信息程度，选择其中信息程度高的作为对象

威胁列表；

行业或业界已有的威胁列表和统计数据；

织发布的关于定级的工业控制系统及其组件面临的威胁；

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；

自志发现的威胁；

可能面临威胁的列表。

2） 查阅企业、

3） 查阅国际组

4） 收集定级的

收集定级的工业控制系统有关现场检测工具收发各

汇集上述威胁信息被综合分析，建立定级的工业控制系统

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

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最高者判定威胁程度特征值（1～5）最高者判定为

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，在

1 中查找对应的高级别，即可确定为工业控制系统信息安全风险

根据 6.1 的要求，用已确定的

抵御的信息安全威胁

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]

[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

[redacted]

区或居[redacted]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，或核设施和铀矿冶设施发生的[redacted]超过[redacted]

[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。

4.2.2.3 较大（Ⅲ级）突发环境事件

[redacted]

2） “国际核事件分级（INES）标准”是由国际原子能机构（IAEA）[redacted]

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[redacted]

[redacted]国防科工委于2001年发布的《国际核事件分级和事件报告系[redacted]

[redacted]

[redacted]织核能机构（OECE/NEA）于[redacted]

件分级（INES）标准对核电厂事件进行分[redacted]

管理办法（试行）》，也使用了国际核事件分

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