ICS 35.040
L 80

中华人民共和国国家标准

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　　2019-10-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

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些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京江南天安科技有限公司、中国电子技术标准化研究院、全球能源互联网研究院有限公司、上海三零卫士信息安全有限公司、网神信息技术(北京)股份有限公司。

本标准主要起草人:陈冠直、邓冬柏、范科峰、高昆仑、周睿康、李琳、梁潇、程鹏、张翀斌、尧相振、龚洁中、李航。

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特征。

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划分规则，规定了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要素，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

信息安全技术
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，并提出了工业控制系统信息安全四个等级的特征。

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。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

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本文件。

3.1.1

信息安全风险 information security risk

特定威胁利用单个或一组资产脆弱性的可能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后果的组合来度量。

[GB/T 31722—2015，定义3.2]

3.1.2

影响 impact

对已建立的业务目标水平的不利改变。在信息安全中，一般指不测事件的后果。

[GB/T 31722—2015，定义3.1]

3.1.3

威胁 threat

可能导致对系统或组织的[illegible]造成损害的不期望事件发生的潜在原因。

[GB/T 29246—2012，定义2.45]

3.1.4

安全属性 security attribute

主体、用户(包括外部的IT产品)、客体、信息、会话[illegible]和/或资源的某些特性，这些特性用于定义安全

功能需求，并且其值用于实施安全功能需求。

[GB/T 25069—2010，定义 2.2.1.18]

3.1.5

可靠性　reliability

预期行为和结果保持一致的特性。

[GB/T 25069—2010，定义 2.1.19]

3.1.6

实时性　real-time

在规定时间内系统获得正确结果的反应能力。

注：一般，实时系统能够及时响应外部事件的请求，并能在一个规定的时间内完成对事件的处理，要求做到逻辑或功能正确(logical or functional correctness)和时间正确(timing correctness)。

3.1.7

信息安全事件　information security incident

一个或一系列意外或不期望的信息安全事态，它/它们极[redacted]能损害业务运行并威胁信息安全。

[GB/T 29246—2012，定义 2.21]

3.2　缩略语

下列缩略语适用于本文件。

DCS：分布式控制系统(Distributed Control System)

ICS：工业控制系统(Industrial control system)

IED：智能电子装置(Intelligent Electronic Device)

PCS：过程控制系统(Process Control System)

[redacted]及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务

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

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)	[illegible]二级(10)
4	4	第二级(7)	[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中的工业控制系统，国家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、电力、天然气、先进制造、水利、[illegible]、环境保护、铁路、城市轨道交通、民航、城市供水供气供热等；

c) 一般领域的工业控制系统：是指上述关键领域和重点领域之外的其他工业生产领域中的工业控制系统。

5.2.1.3 工业控制系统资产作用价值

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、受依赖程度等情况，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) 当工业控制系统控制对象属于工业生产系统的核心生产部位，该控制对象功能受到损害或丧失会对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，当该工业控制系统功能受到损害或丧失时，工业生产系统无法运行或不能正常运行，甚至会发生危险，而且无法通过手工操作辅助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总值很高。

b) 资产作用价值中等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重要业务使命；

2) 当工业控制系统控制对象属于工业生产系统的重要生产部位，该控制对象功能受到损害或丧失会对局部生产流程产生中断或主要生产流程产生较大影响；

3) 工业生产系统对该工业控制系统的依赖程度中等，当该工业控制系统功能受到损害或丧失时，工业生产系统部分不能正常运行但不会发生危险，而且可通过手工操作辅助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总值中等。

c) 资产作用价值一般的工业控制系统

依据制造国内相关工业生产装置设施价值

2） 工业控制系统设备本身更换或再造成本一般，或者因事件导致系统可用性、完整性和保密性的损失，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准确顺序或协调性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习惯确定。

5.2.2 受侵害后的潜在

5.2.2.1 受侵害后潜在影响程度

安全等级的定级要素之一，由受侵害的对象(5.2.2.2)

资产丧失[illegible]或后果，可能影响到一项或多项资产和业务过程，或者资产也可能是永久性的(当资产被毁灭时)。

侵害后潜在影响程度特征值表示，如表3所示：

害后潜在影响程度特征值

	受侵害的程度		
	一般损害	严重损害	特别严重损害
	1	2	3
企业、[illegible]	[illegible]	[illegible]	[illegible]
[illegible]安全	[illegible]	[illegible]	[illegible]
益、命安全	2	3	4
[illegible]	[illegible]	4	5
经济[illegible]	[illegible]	[illegible]	[illegible]

适用从1～5，工业控制系统受侵害后潜在影响程度越高。

受侵害后潜在影响程度是工业控制系统信息和受侵害的程度(5.2.2.3)确定。

当工业控制系统信息安全受到侵害，因其统本身和其他相关受侵害的对象造成的损害和业务过程的一部分；后果可能是临时性的工业控制系统信息安全受侵害程度用受

表3 受侵

受侵害后潜在影响程度	
受侵害的对象	工业控制系统及相关生产装置安全
	工业生产运行安全和公民[illegible]组织合法权益[illegible]
	社会秩序、公共环境安全和人员生
	国家安全（特别是其中的国家

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

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。这些受侵害的对象可划分如下：

a) 工业控制系统及相关生产装置安全；

b) 工业生产运行安全和公民、企业、其他组织的合法权益及重要财产安全；

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[7])。

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、完整性、保密性等三个安全目标受到侵害。通常，工业控制系统信息安全受到侵害时，可用性、完整性、保密性的可能影响值并非总是相同的，应以三个安全目标中受到[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]控制系统信息安全受到破坏后，因其资产丧失可用性、完整性和保密性等事件分别会造成不同程度的损害或后果，选择各个受侵害对象的受侵害程度中最大的，确定其受侵害程度。受侵害的程度划分如下：

[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，通常有：

1) 意外的威胁，是指非恶意人员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，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) 故意的威胁，是指恶意人员故意地损害工业控制系统资产的所有行为，如心怀不满的在职员工、无特殊诉求的黑客、心怀不满的离职人员、经济罪犯、恐怖分子、敌对势力或敌对国家的恶意行为等；

3) 环境的威胁，是指非人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一个或多个属性，而资产正是通过这些属性来体现价值的。常见的威胁表现形式主要有：

1) 被动信息收集：可为潜在入侵者提供有价值的信息；

4) 对手：是指某占有中等程度资源且愿意冒较大风险的熟练对手的故意威胁（如敌对组织

严重的环境威胁、特别严重的意外威胁，以及其他相关类

对于战争威胁，包括来自国家级别暴力手段的威胁，以及毁灭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等级确定条件中，信息安全事件发生的可能性是指，工业控制系统面临特定信息安全威胁源发生相应信息安全事件可能性的高低。工业控制系统某个信息安全事件可能性，应通过特定威胁发生可能性以及脆弱性利用容易度组合来评价。其中：

a) 根据 5.2.3.2 中的要求建立威胁列表，并对每个威胁逐一分析其发生频度；

b) 识别定级的工业控制系统存在的固有脆弱性及其相关因素；

c) 对威胁列表中每个威[illegible]

对于工业控制系统信息安全事件可能性的评价，应综合工业控制系统对于威胁发生可能性与脆弱程度确定，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，第一级应具有以下主要特征：

a) 第一级工业控制系统信息安全受到破坏后，会对一般领域的工业生产运行造成损害，或者对公[illegible]

[illegible]安全控制措施，检测系统异常和安全事件，应急响应的执[illegible]

[illegible]系统，运行环境安全风险的比较全面认识，初步建立[illegible]全控制措施；及时检测系统异常和安全事件；应急响应[illegible]；基本恢复受安全事件[illegible]

c) 第二级工业控制系统应至少具有对系统[illegible]风险管理战略；采取比较全面的信息安[illegible]的执行和维护，防止事件扩大和减轻影[illegible]

面的安全保护能力；

d) 第二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保护和管理，以及国家主管部门和信息安全监管部门的指导。

5.3.3 第三级工业控制系统

按照基于风险评估的信息安全等级划分的工业控制系统，第三级应具有以下主要特征：

a) 第三级工业控制系统信息安全受到破坏后，会对重点领域的工业生产运行造成重大损害，或者对关键领域的工业生产运行造成损失，或者对环境安全、社会秩序、公共利益和人员生命造成严重损害，或者会对国家安全（特别是其中的国家经济安全）造成损害；

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源的故意威胁，严重的环境威胁，特别严重的意外威胁，以及其他相当危害程度威胁所造成资产损失的信息安全风险；

c) 第三级工业控制系统应至少具有对系统资产、运行环境、安全风险的全面认识，建立风险管理战略，实施信息安全治理，采取全面的信息安全控制措施，确保与组织的风险管理战略相一致；及时和全面监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；恢复受安全事件影响的工业控制系统运行方面的安全保护能力；

d) 第三级工业控制系统信息安全应得到所属企业依据国家有关

业控制系统信息安全定级流程是一致的。定级流程中的确定工业控制系统定级对象，是在建立风险评估的语境；定级流程中的确定工业控制系统资产重要程度、确定受侵害后的潜在影响程度、确定需抵御的信息安全威胁程度，属于风险分析的风险识别及部分风险估算活动；定级流程中的确定工业控制系统信息安全等级，属于风险评价活动。

确定工业控制系统作为定级对象的工业控制系统信息安全等级的一般流程如图 1 所示：

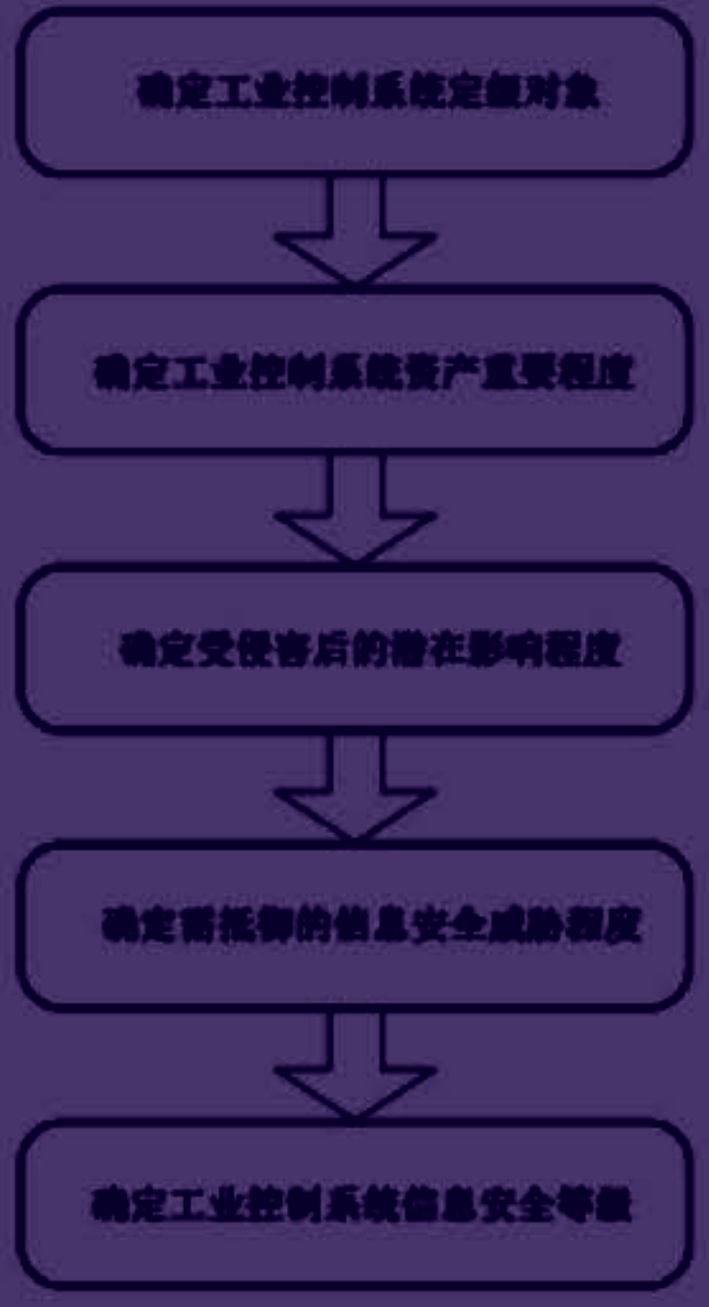

图 1　工业控制系统信息安全定级流程

6.2　确定工业控制系统定级对象

6.2.1　定级对象的确认条件

确认一个工业控制系统作为定级对象，该工业控制系统应具备如下基本条件：

a）　一个具体的定级的工业控制系统

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） 具有工业控制系统的基本要素：

1） 作为定级对象的工业控制系统应该是由相关的自动化控制组件以及对实时数据进行采集、监测的过程控制组件按照一定的工业控制目标、控制流程和控制规则组合而成的有形实体，保留完整[illegible]

[illegible]

[illegible]

[illegible]

[illegible]部署：包括工业控制系统的物理环境、工业控制系统网络拓扑结构、工业控制系统及受控设备的部署情况，并明确工业控制系统的边界。

工业控制系统的业务种类和特性：包括工业控制系统涉及的业务种类和受控[illegible]数量，以及工业控制系统对可用性、实时性、可操作性、完整性、保密性需求及业务特性，如是否形成闭合控制回路、是否为连续控制系统等。

d） 工业控制系统[illegible]系统服务：包括为完成预定的业务目标和任务，提供的操作、控制过程和其他业务功能，以及这些服务在可用性（如及时有效）、完整性和保密性等方面的重要性。

e） 工业控制系统的业务数据：包括工业控制系统涉及的主要[illegible]及相关协议，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[illegible]与企业相关信息系统的连接：包括连接方式、接口控制、传输内容，及相关用户范围和用户类型等。

g） 工业控制系统的管理框架：包括工业控制系统的组织管理结构、管理策略、相关部门设置和部门在业务运行中的作用、岗位职责。

h） 比较大的或复杂的工业控制系统的安全区域和通讯网络作为定级对象，应描述与相关安全区域和通讯网络的相互依赖关系。

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 的要求，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属于以下类型之一：
   1) 一般资产价值；
   2) 很高资产价值。
b) 按照 5.2.1.2 的要求，对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) 一般领域；
   2) 重点领域；
   3) 关键领域。
c) 按照 5.2.1.3 的要求，对工业控制系统在工业生产系统中所具有的业务使命进行分析，确定该工业控制系统的业务使命属于以下类型之一：
   1) 一般业务使命；
   2) 重要业务使命；
   3) 关键业务使命。

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，分析工业控制系统资产重要性相关内容，依照表 2 得出工业控制系统资产重要程度待定值，取值范围是低到高[illegible]共 5 个等级。

6.4 确定受侵害后的潜在影响程度

6.4.1 确认工业控制系统信息安全受到破坏

工业控制系统信息安全主要包括保护、维[illegible]

列破坏的情况，并选择其中受列破坏最严重

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） 影响各种类型的经济活动秩序；

3） 影响各行业的科研、生产秩序；

4） 影响公众在法律约束和道德规范下的正常生活秩序等；

5） 其他影响社会秩序稳定的事项。

d） 侵害公共利益的事项：

是指定级的工业控制系统信息安全受到侵害，及其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） 影响社会成员接受公共服务等方面；

5） 其他影响公共利益及重要公共财产安全的事项。

e） 侵害环境安全和人民生命安全的事项：

是指定级的工业控制系统信息安全受到侵害，及其造成工业生产系统受到侵害，并由此产生对环境安全的影响，主要包括以下方面：

1） 影响工业控制系统及工业生产系统的生产技术性环境、相关自然生态环境，造成污染或破坏；

2） 因环境污染或破坏直接导致人员死亡或中毒、造成人员的散转移、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绝、造成集中式饮用水水源地取水中断、造成严重辐射污染后果等。

f） 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受到侵害，及其造成工业生产系统受到侵害，并由此产生对公民、企业和其他组织的合法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；

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，直接或间接造成的轻伤或死亡等伤害。

g） 侵害工业生产运行安全的事项：

是指定级的工业控制系统信息安全受到侵害，直接产生对其控制范围内的以及上下游相关的工业生产运行安全的影响，主要包括以下方面：

1） 影响工业生产运行的有关过程不能正常；

2） 影响工业生产运行的正常连续性，出现运行中断；

3） 影响工业生产运行安全，发生生产安全事故，甚至影响人员生命财产安全。

h） 侵害工业控制系统自身功能受到损害或丧失的事项：

是指定级的工业控制系统信息安全受到侵害，及其造成工业控制系统自身功能受到损害或丧失，并由此产生对其所控制的相关生产装置功能受到损害或丧失，以致影响工业生产运行安全，主要包括以下方面：

1） 工业控制系统自身功能不能正常；

2） 工业控制系统自身功能完全丧失；

3） 工业控制系统自身受到毁坏；

4） 工业控制系统相关生产装置功能不能正常；

5） 工业控制系统相关生产装置功能受到损害或丧失；

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的损失，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]

当工业控制系统信息安全受到破坏时，造成对环境安全和人员生命安全的侵害程度，可通过生产安全事故和突发环境事件的等级表述，判定条件如下：

a) 生产安全事故等级：根据国务院第 493 号令中规定的条件（见附录 A 中 A.1），确定为下列等级之一：

1) 特别重大事故；

2) 重大事故；

3) 较大事故；

4) 一般事故。

b) 突发环境事件等级：根据环境保护部令第 17 号中规定的条件（见附录 A 中 A.2），确定为下列等级之一：

1) 特别重大（Ⅰ级）突发环境事件；

2) 重大（Ⅱ级）突发环境事件；

4） 对工业生产系统运行的地理区域、人群区域、生产生活领域之外的时间跨度影响较小；

5） 不会发生生产安全事故或突发环境事件。

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 提供的方法，判[illegible]会秩序稳定的侵害程度；按照 6.4.4.4 提供的[illegible]

[illegible]的对受侵害对象的侵害程度按照下列受侵害程度之一表示：

——造成一般损害；

——造成严重损害；

——造成特别严重损害。

根据 a）判定的一个或几个受侵害对象，以及根据 b）判定的对相应受侵害对象的侵害程度，逐[illegible]按照 5.2.2.4 的要求，分析工业控制系统受侵害后潜在影响的相关内容；分别依照表 3 得出工业控制系统受侵害潜在影响程度特征值，并选择其中最高者作为工业控制系统受侵害潜在[illegible]

评价工业控制系统面临的信息安全威胁，包括：

a） 分析定级的工业控制系统可能面临的各种威胁，如：

1） 按照 5.2.3.2 列出的常见威胁列表；

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[illegible]在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日志发现的威胁；

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确定其特征值（取值范围为 1～5），形成定级的工业控制系统完整的威胁列表。

6.5.2 评价信息安全事件可能性

评价信息安全事件可能性的目的是识别威胁和估算其发生可能性，应考虑来自事件和以往威胁评估的内部经验，关注相关威胁的持续变化，特别是当业务环境或工业控制系统发生变化时。评价信息安全事件可能性包括：

a） 根据 6.5.1 形成的威胁列表，对确定存在的每一种威胁逐一分析其发生频度：

1） 收集定级的工业控制系统以往安全事件报告中、各种日志中或现场检测工具发现的威胁发生的频度；

2） 收集行业[illegible]或企业[illegible]内类似工业[illegible]控制系统的[illegible]威胁发生的频度；

3） 收集国际组织发布的类似工业控制系统的威胁发生的频度；

4） 其中，威胁发生频度分为高、中、低，对没有发生过定为发生频度低，发生过1次定为发生频度中，发生过多次定为发生频度高；

5） 选择1）～3）中发生频度的最高者作为定级的工业控制系统对该指定威胁发生的频度。

b） 识别工业控制系统存在的固有脆弱性，即工业控制系统、相关生产装置以及所属企业或行业本身固有的，而非某个工业控制系统个体原因（如人为疏忽）造成的脆弱性，如：

1） 用于易燃易爆、强辐射、剧毒等危险品生产的工业控制系统；

2） 用于野外或难以监管的工业控制系统；

3） 受行业生产条件限制或技术水平限制，存在一定缺陷的业工业控制系统；

4） 工业控制系统所属企业或行业固有的单个和聚集的脆弱性；

5） 对意外的威胁或环境的威胁，如地理因素、极端天气情况的可能性、可能导致人为错误或设备故障的因素；

6） 应关注工业控制系统固有脆弱性可利用容易度的变化，当环境变化、技术变化、系统部件的故障，替换部件的不可用、人员流动、以及更高级的威胁出现的影响，一个最初只[illegible]有限固有脆弱性的工业控制系统，[illegible]。

c） 识别工业控制系统存在固有脆弱性的相关因素：

1） 工业控制系[illegible]资产的吸引力或可能影响[illegible]

数值(或值范围)为

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

A.1　生产安全事故分级

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）标准”属于4级以上的核事故；周边国家核设施中发生的按照“国际核事件分级（INES）标准”属于4级以上的核事故；

g) 跨国界突发环境事件。

A.2.2.2 重大（Ⅱ级）突发环境事件

凡符合下列情形之一的，为重大突发环境事件：

a) 因环境污染直接导致3人以上10人以下死亡或50人以上100人以下中毒的；
b) 因环境污染需疏散、转移群众1万人以上5万人以下的；
c) 因环境污染造成直接经济损失2 000万元以上1亿元以下的；
d) 因环境污染造成区域生态功能部分丧失或国家重点保护野生动植物种群大批死亡的；
e) 因环境污染造成县级城市集中式饮用水[illegible]
f) [illegible]弃、遗撒危险废物等造成的突发环境事件发生在国家重点流域、国家级自然保护区、风景名胜区或居民聚集区、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达到进入场区应急状态标准的，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。

A.2.2.3 较大（Ⅲ级）突发环境事件

[illegible]

[illegible]与发展组织核能机构[illegible]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[illegible]级。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[illegible]级（INES）标准。

(OECE/NEA)于
电厂事件进行分
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—2012 信息技术 安全技术 信息安全管理体系 概述和词汇
[5] 关于加强工业控制系统信息安全管理的通知 工信部协[2011]451号
[6] IEC 62443 Security for industrial automation and control systems