



中华人民共和国国家标准

GB/T 36324—2018

信息安全技术 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 发布
中国国家标准化管理委员会

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 5

 5.3 工业控制系统信息安全等级特征 10

6 工业控制系统信息安全等级定级方法 11

 6.1 工业控制系统信息安全定级流程 11

 6.2 确定工业控制系统定级对象 14

 6.3 确定工业控制系统资产重要程度 14

 6.4 确定受侵害后的潜在影响程度 14

 6.5 确定需抵御的信息安全威胁程度 20

 6.6 确定工业控制系统信息安全等级 22

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 23

参考文献 25

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、国家经济安全和社会公共安全,为切实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,提出了工业控制系统信息安全定级流程,陈述了确定工业控制系统定级对象、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、确定工业控制系统信息安全等级;附录A说明了有关生产安全事故和突发环境事件分级。

在5.3中,为清晰表示工业控制系统每一个信息安全等级比较低一级安全等级的安全技术要求的增加和增强,每一级的新增部分用“宋体加粗字”表示。

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,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

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

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,可独立构成工业控制系统的

图 17

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)				

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、

c) 一般领域的工业控制系统:是指除上述关键领域和重点领域以外的工业控制系统,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,该控制对象功能受损或丧失不会对主要生产流程产生影响或影响较小;
- 3) 工业生产系统对该工业控制系统的依赖程度低,当该工业控制系统功能受到损害时,可改为手工操作,并能通过其他控制手段保证工业生产系统持续运行。

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对象

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工业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:

- a) 造成一般损害;
- b) 造成严重损害;
- c) 造成特别严重损害。

5.2.3 需抵御的信息安全威胁

5.2.3.1 需抵御的信息安全威胁程度

需抵御的信息安全威胁程度是工业控制系统信息安全等级的定级要素之一,由工业控制系统面临的信息安全威胁(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;
- b) 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“低”时,则该信息安全威胁可舍去,即确认为不需要抵御的威胁;
- c) 通过取舍后,在实际需要抵御的众多信息安全威胁中,确定该工业控制系统的最高的信息安全威胁程度待估值。

对于信息安全威胁造成工业控制系统信息安全事件发生可能性高低的界限,应依据各个工业生产行业对安全事件可能性的敏感程度确定。当不能依据各个工业生产行业对安全事件可能性的敏感程度确定时,

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。

对于战争威胁,包括来自国家级暴力手段的威胁,以及毁灭性自然灾害等意外威胁,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,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:

- 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;
- 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;
- 对威胁列表中每个威胁,分析其发生的可能性,并考虑脆弱性利用容易度,综合评估信息安全事件发生的可能性。

根据上述分析,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:

- 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,或者对公民、企业和其他组织的合法权益及重要财产造成损害,但不会损害国家安全(特别是其中的国家经济安全)、环境安全、社会秩序、公共利益和人员生命;

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、拥有少量资源的故意威胁,一般的环境威胁,一般的意外威胁,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;

第一级工业控制系统至少应具有对系统资产、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,应急响应的基本能力和维护等方面的安全保护能力;

- 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关管理规范和技术标准的保护和管理。

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,第二级应具有以下主要特征:

- 第二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);

- 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、拥有中等资源的故意威胁,一般的环境威胁,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;

第二级工业控制系统应至少具有对系统资产、运行环境、安全风险的基本认识,制定信息安全风险管理战略,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影响的工业控制系统运行等方面

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,确保与信息安全风险管理战略相一致;

及时和全面监测系统异常;

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

确定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:

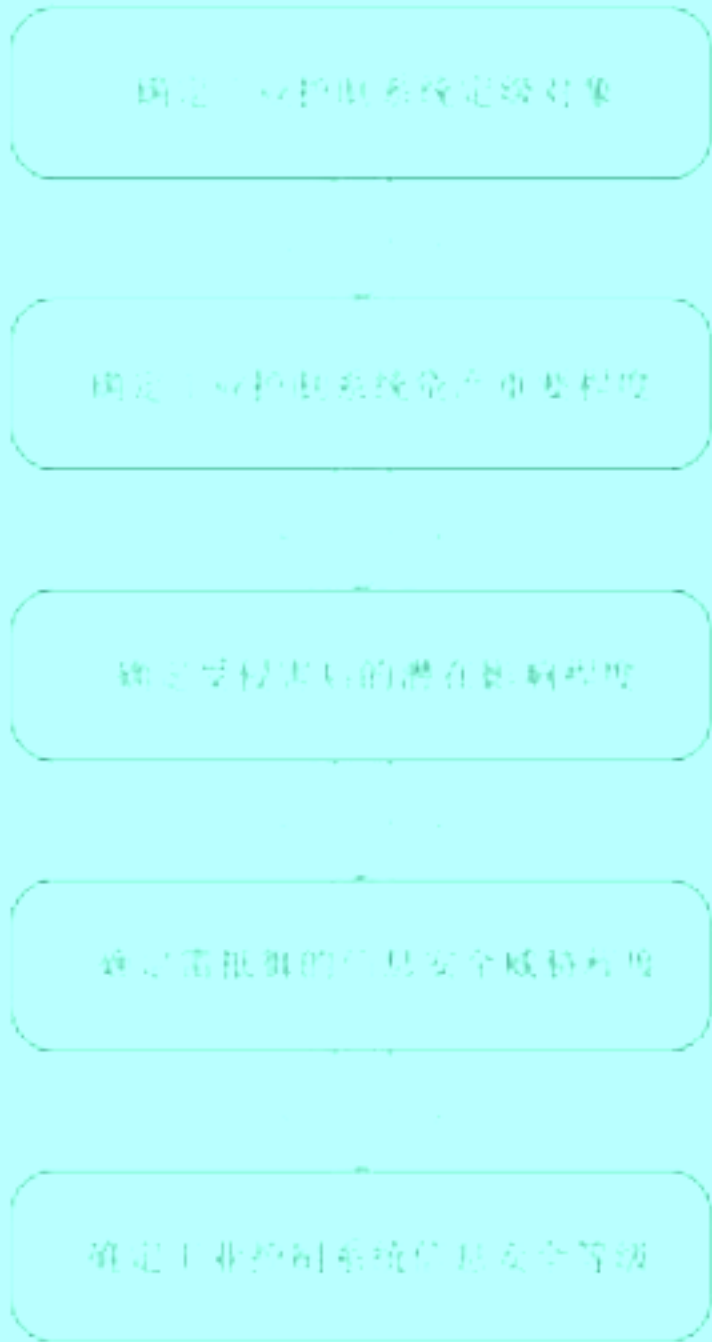


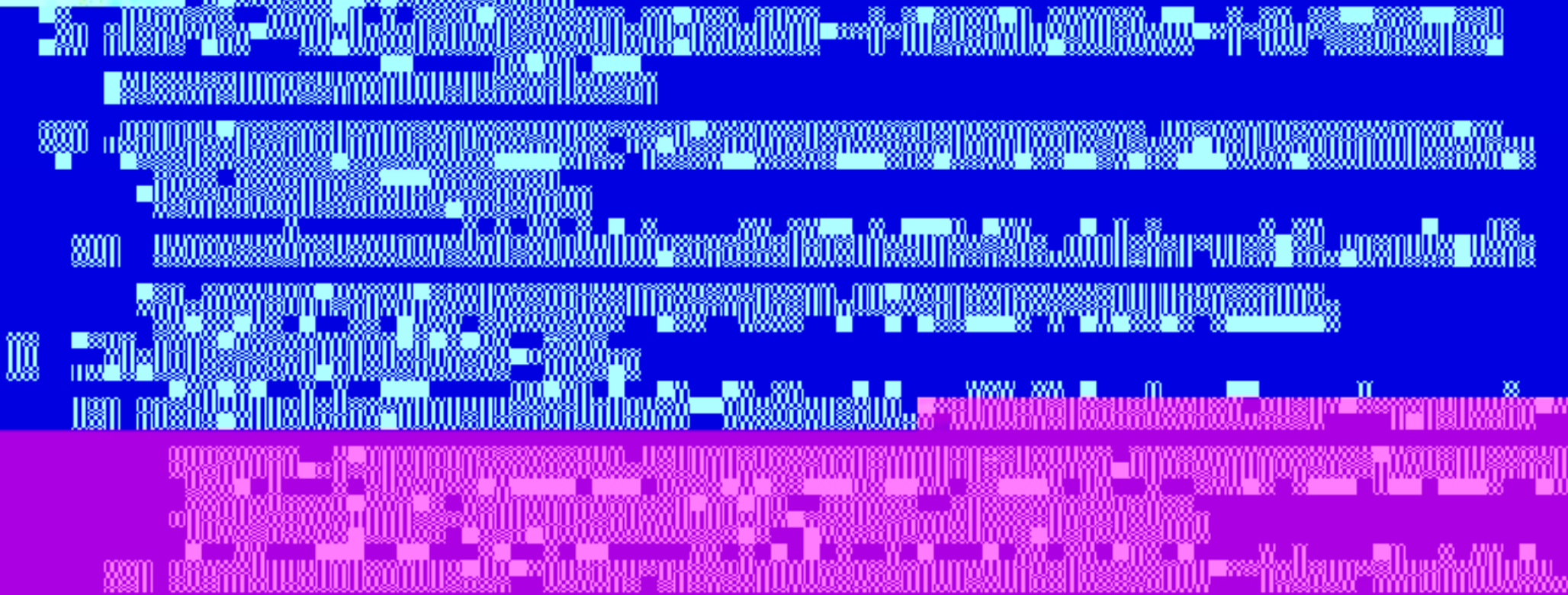
图 1 工业控制系统信息安全定级流程

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) 一个具独立功能的工业控制系统;



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控制组以及对实时数据进行采

米、面粉的总性控制组只按照一定的工业控制目标、控制流程和控制频率组合而成，没有实体，保留完整。

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特征值,取值范围是低到高(1~5),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、维持、恢复、利用、删除、传输、交换、披露、发布、

完整性、保密性属性的部分或全部受到破坏。在确认工业控制系统信息安全受到破坏中,需要分别查看这三个方面安全属性受

分或全部受到破坏。在确认工业控制系统信息安全受到破坏中,需要分别查看这三个方面安全属性受

到破坏时粘附，并逐板取出至到破坏时呈亚

目次

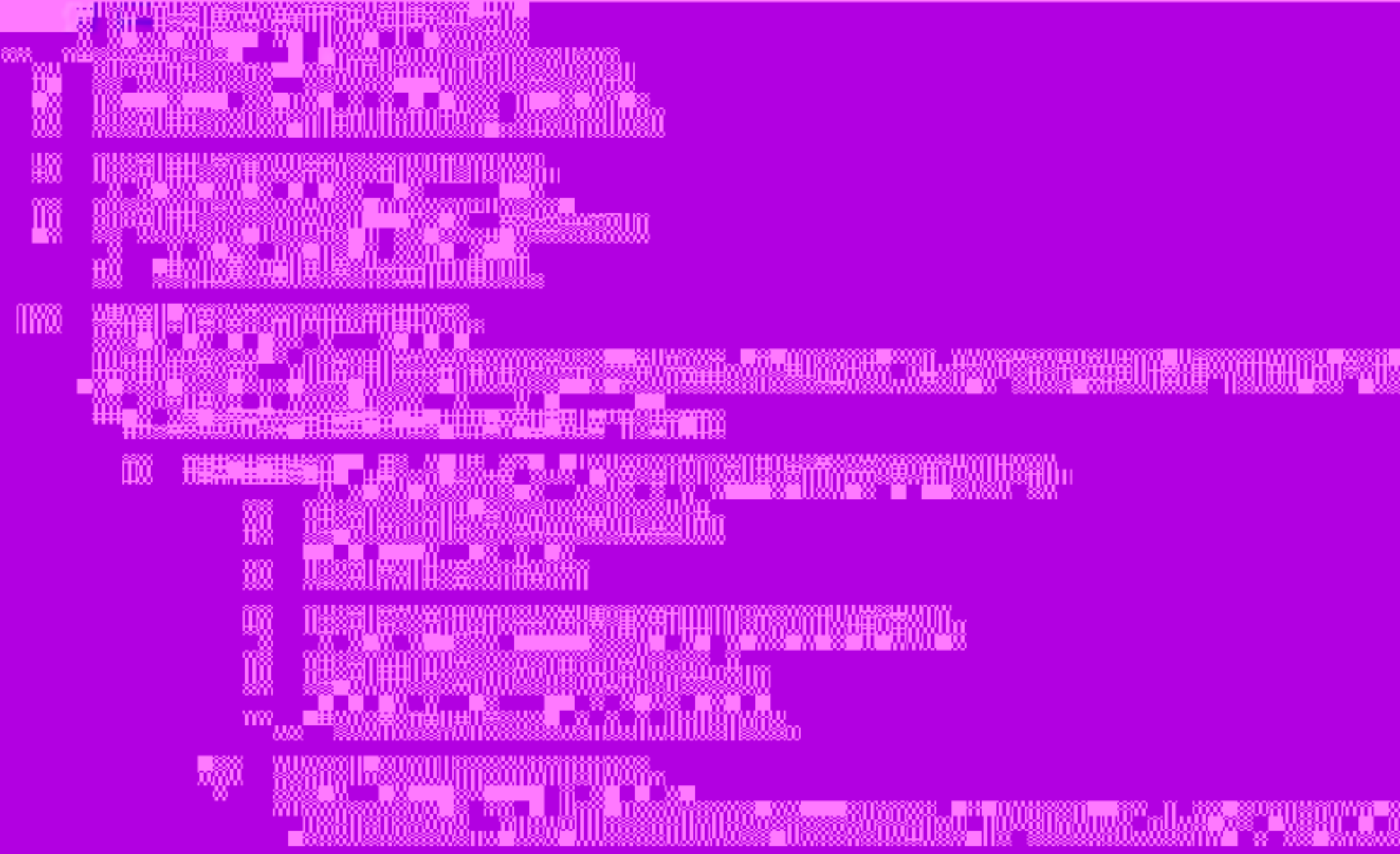
0 引言

1 范围

2 规范性引用文件

3 术语和定义

3 术语和定义



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重要财产安全的影响,主要包括以下方面:

- 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;
- 6) 工业控制系统相关生产装置受到毁坏。

6.4.4 评价受侵害的程度

6.4.4.1 判定对国家安全的侵害程度

当工业控制系统信息安全受到破坏

[illegible][illegible][illegible]

110228

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was significantly higher than the number of incorrect responses for all groups. The number of correct responses was significantly higher than the number of incorrect responses for all groups. The number of correct responses was significantly higher than the number of incorrect responses for all groups.

[illegible]



www.pearsoned.com

[illegible]

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大范围的社会不良影响,对重要公共财产造成极高损失,可判定对公共利益、重要公共财产的侵害程度为特别严重损害。

6.4.4.5 判定对环境安全和人员生命安全的侵害程度

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;
 - 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、企业和其他组织的合法权益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,判定条件如下:

- a) 一般损害:当对公民、企业、其他组织的工作职能产生局部影响,业务能力有所降低但不影响主要功能的执行,出现较轻的法律问题,以及较低的财产损失时,可判定对公民、企业、其他组织的合法权益及重要财产安全的侵害程度为一般损害;
- b) 严重损害:当对公民、企业、其他组织的工作职能产生严重影响,业务能力显著下降且严重影响主要功能执行,出现较严重的法律问题,以及较高的财产损失时,可判定对公民、企业、其他组织的合法权益及重要财产安全的侵害程度为严重损害;
- c) 特别严重损害:当对公民、企业、其他组织的工作职能产生特别严重影响,业务能力完全丧失且严重影响主要功能执行,出现特别严重的法律问题,以及特别高的财产损失时,可判定对公民、企业、其他组织的合法权益及重要财产安全的侵害程度为特别严重损害。

- 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。
- b) 严重损害:判定对工业生产系统运行安全的侵害程度为严重损害的条件为:
- 1) 对工业生产系统的大部分任务不能完成或整体功能严重下降;
 - 2) 出现部分系统的功能严重下降或产生中断,出现的故障不能立即通过检修予以修复。

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) 按照附录4.3提供的方法，判定系统运行过程确定的侵害程度；按照附录4.3提供的方

6.5.2 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（或企业）内类似工业控制系统的威胁发生频度；

- 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,一个最初只有有限固有脆弱性的工业控制系统,可能会变得更易受攻击。



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

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

国务院

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水源地取水中断的;

注:1) 核设施是指核动力厂、核燃料元件制造厂、核燃料元件后处理厂、核动力厂乏燃料元件贮存设施、研究堆、实验堆、放射性废物集中贮存设施、放射性废物处置场等设施的统称;核设施内发生的核事故是指核动力厂内发生的可能造成放射性物质外泄,并导致放射性物质释放到环境中的事故。核设施内发生的核事故按国际核事件分级(INES)标准分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

2) 按照《国际核事件分级表》,核事件按放射性物质外泄量、放射性物质对公众健康、环境及财产造成的危害程度分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

3) 跨省(区、市)突发环境事件。

A.2.2.3 较大(Ⅲ级)突发环境事件

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5万人以上10万人以下的;
- c) 因环境污染造成直接经济损失1 000万元以上2 000万元以下的;
- 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死亡的;
- e) 因环境污染造成设区的市级城市集中式饮用水水源地取水中断的;

注:1) 核设施是指核动力厂、核燃料元件制造厂、核燃料元件后处理厂、核动力厂乏燃料元件贮存设施、研究堆、实验堆、放射性废物集中贮存设施、放射性废物处置场等设施的统称;核设施内发生的核事故是指核动力厂内发生的可能造成放射性物质外泄,并导致放射性物质释放到环境中的事故。核设施内发生的核事故按国际核事件分级(INES)标准分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

2) 按照《国际核事件分级表》,核事件按放射性物质外泄量、放射性物质对公众健康、环境及财产造成的危害程度分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

3) 跨省(区、市)突发环境事件。

凡符合下列情形之一的,为一般突发环境事件:

- a) 因环境污染直接导致3人以下死亡或10人以下中毒的;
- b) 因环境污染需疏散、转移群众5万人以上10万人以下的;
- c) 因环境污染造成直接经济损失1 000万元以上2 000万元以下的;
- 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死亡的;
- e) 因环境污染造成设区的市级城市集中式饮用水水源地取水中断的;

注:1) 核设施是指核动力厂、核燃料元件制造厂、核燃料元件后处理厂、核动力厂乏燃料元件贮存设施、研究堆、实验堆、放射性废物集中贮存设施、放射性废物处置场等设施的统称;核设施内发生的核事故是指核动力厂内发生的可能造成放射性物质外泄,并导致放射性物质释放到环境中的事故。核设施内发生的核事故按国际核事件分级(INES)标准分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

2) 按照《国际核事件分级表》,核事件按放射性物质外泄量、放射性物质对公众健康、环境及财产造成的危害程度分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

3) 跨省(区、市)突发环境事件。

凡符合下列情形之一的,为一般突发环境事件:

- a) 因环境污染直接导致3人以下死亡或10人以下中毒的;
- b) 因环境污染需疏散、转移群众5万人以上10万人以下的;
- c) 因环境污染造成直接经济损失1 000万元以上2 000万元以下的;
- 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死亡的;
- e) 因环境污染造成设区的市级城市集中式饮用水水源地取水中断的;

注:1) 核设施是指核动力厂、核燃料元件制造厂、核燃料元件后处理厂、核动力厂乏燃料元件贮存设施、研究堆、实验堆、放射性废物集中贮存设施、放射性废物处置场等设施的统称;核设施内发生的核事故是指核动力厂内发生的可能造成放射性物质外泄,并导致放射性物质释放到环境中的事故。核设施内发生的核事故按国际核事件分级(INES)标准分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

2) 按照《国际核事件分级表》,核事件按放射性物质外泄量、放射性物质对公众健康、环境及财产造成的危害程度分为7级,其中1~3级核事件属于一般核事件,4~7级核事件属于重大核事件。

3) 跨省(区、市)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—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
-