ICS 35.040
L 80

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
中国国家标准化管理委员会　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 …… 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 …… 12
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

事件的后果，对已达到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、会话和/或资源的某些特性，这些特性用于定义安全