ICS 35.240.50
CCS L62

团 体 标 准

T/XXX XXXX—XXXX

工业信息安全漏洞分类分级指南

Guidelines for classification of industrial information security vulnerability

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国和平利用军工技术协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国和平利用军工技术协会提出并归口。

本文件起草单位：

本文件主要起草人：

工业信息安全漏洞分类分级指南

1 范围

本文件提供了工业信息安全漏洞的分类方法、分级指标及可行的分级方法等建议。

本文件适用于工业领域的软硬件产品提供者、工业信息安全漏洞收集组织、工业信息安全漏洞应急组织在漏洞管理、技术研发等活动中的漏洞分类和分级评估，工业领域产品提供者、工业领域产品运营者的漏洞分类和漏洞分级可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 30279 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 30279 界定的以及下列术语和定义适用于本文件。

3.1

工业信息安全 industrial information security

工业运转过程中的信息安全。

注：工业信息安全涉及工业领域各个环节，直接关系到经济进展与社会稳定。包括工业控制系统安全、工业互联网安全、工业大数据安全、工业云安全、工业电子商务安全、关键信息基础设施安全等领域。

3.2

工业信息安全漏洞 industrial information security vulnerability

在整个工业运转过程中，存在于工业领域专有的、非通用信息技术的软件、硬件、协议、系统中，对工业信息、工业领域各个环节甚至经济进展与社会稳定造成影响的漏洞。

3.3

受影响实体 impacted entity

工业信息安全漏洞触发时，其直接影响的工业领域专有硬件、协议、软件、系统等具体实体对象。

注：如某可编程逻辑控制器、某工业控制协议、某工业控制软件等。

4 缩略语

下列缩略语适用于本文件。

APP：移动智能终端应用软件（Application）
DCS：集散控制系统（Distributed Control System）
DTU：数据传输单元（Data Transfer unit）
I/O：输入/输出（Input/Output）
OLE：对象连接与嵌入（Object Linking and Embedding ）
OPC：对象链接与嵌入的过程控制（OLE for Process Control）
PLC：可编程逻辑控制器（Programmable Logic Controller）
RTU：远程终端单元（Remote Terminal Unit）
SQL：结构化查询语言（Structured Query Language）
WEB：全球广域网或万维网（World Wide Web）

5 工业信息安全漏洞分类

5.1 概述

本文件提供了工业信息安全漏洞的分类依据，并划分工业信息安全漏洞类型。本文件采用受影响实体和漏洞成因两种分类方法对工业信息安全漏洞进行划分。

5.2 按受影响实体分类

5.2.1 工业生产控制设备

工业生产控制设备指工业控制的各种生产控制设备/系统，包括但不限于：工业传感设备、工业机器人、DCS、PLC、可编程自动化控制器、RTU、现场总线系统、数控机床、智能仪表系统、许可认证服务器、变频器、伺服系统、DTU等。

5.2.2 工业网络通信设备

工业网络通信设备指用于工业环境下的通信设备，包括但不限于：工业交换机、工业路由器、工业网关、串口服务器、光纤收发器、工业无线接入点、工业无线控制器等。

5.2.3 工业主机设备和软件

工业主机设备和软件指用于工业领域的终端、控制系统及软件，包括但不限于：嵌入式系统、数据采集与监控系统、操作员面板、OPC服务器、工业软件、组态软件、工业主机、工业数据库等。

5.2.4 工业生产信息系统

工业生产信息系统指用于工业生产管理所使用的系统，包括但不限于：制造执行系统、企业资源规划、产品生命周期管理系统、实验室信息管理系统、能源管理系统、仓库管理系统、供应链管理系统、工业云平台、工业APP等。

5.2.5 工业网络安全设备

工业网络安全设备指为工业网络提供安全防护、监测、分析的设备或平台，包括但不限于：工业防火墙、工业网闸、工业主机安全防护设备等。

5.2.6 物联网智能设备

物联网智能设备指物联网领域的智能设备，包括但不限于：安防监控设备、智能家居设备、智能穿戴设备、车联网设备、智能医疗设备、无人机等。

5.2.7 楼宇自动化控制系统

楼宇自动化控制系统指楼宇自动化的监管与管理系统，包括但不限于：数字控制器、空调与通风监控系统、给排水监控系统、照明监控系统、电梯运行监控系统、综合保安系统、消防监控系统、结构化综合布线系统、电力供应监控系统等。

5.2.8 定位、授时、导航系统

定位、授时、导航系统指导航、定位、时钟同步等的软硬件产品，包括但不限于：时钟控制系统、导航系统等。

5.2.9 其他

其他上述未涵盖的所有应用于工业控制、工业互联网、物联网、车联网等领域的设备、系统、软件、协议等软硬件产品。

5.3 按漏洞成因分类

5.3.1 通则

工业信息安全漏洞按漏洞成因分类是指在5.2中受影响实体中漏洞产生或触发的技术原因，漏洞成因分类架构见图1。

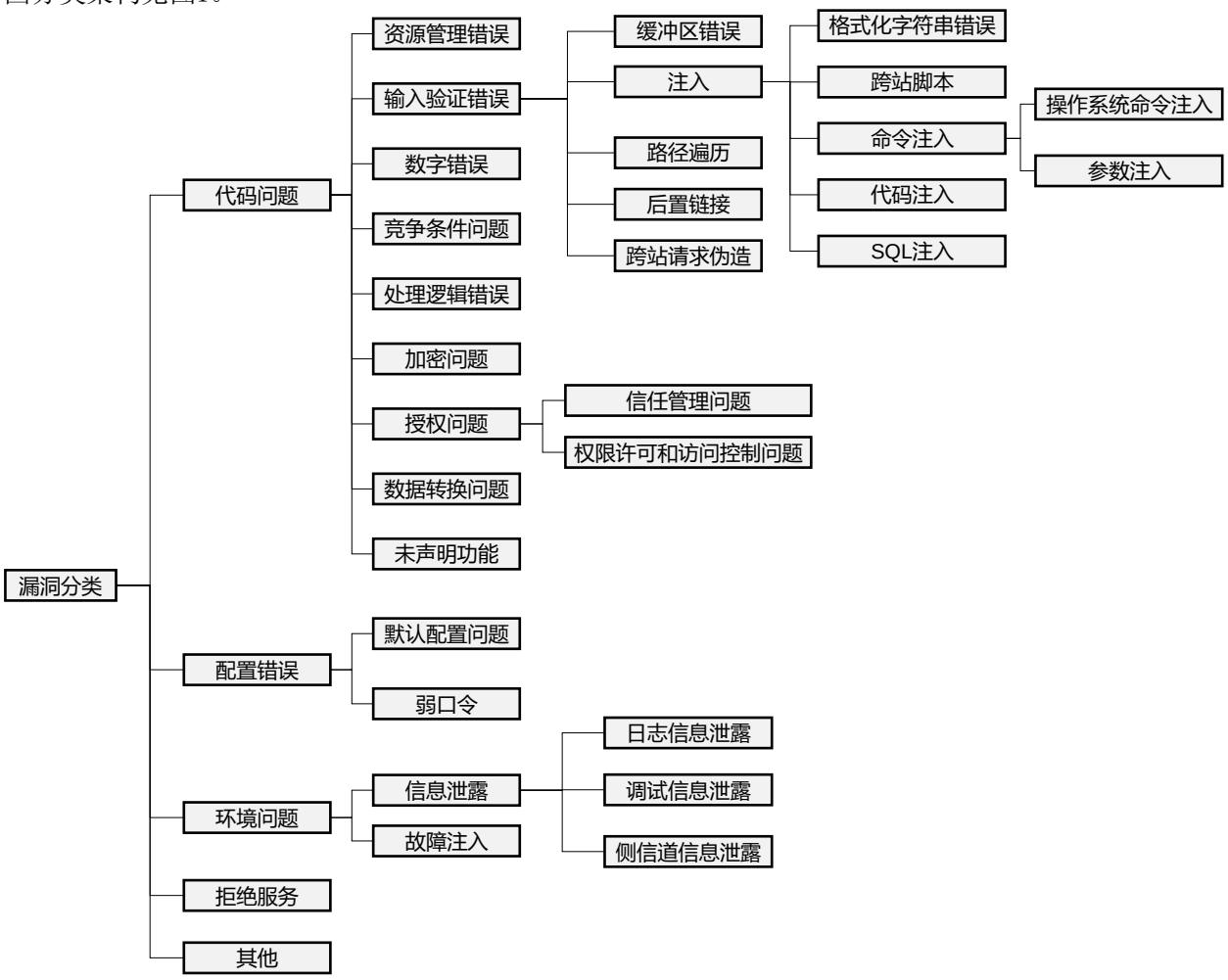

图1 漏洞成因分类导图

5.3.2 代码问题

5.3.2.1 概述

代码问题漏洞指受影响实体的代码开发过程中因设计或实现不当而产生的漏洞。

5.3.2.2 资源管理错误

资源管理错误漏洞指因对内存、磁盘空间、文件等受影响实体资源的错误管理造成的漏洞。

5.3.2.3 输入验证错误

5.3.2.3.1 概述

输入验证错误漏洞指受影响实体因对输入的数据缺少正确、完备的验证而产生的漏洞。

5.3.2.3.2 缓冲区错误

缓冲区错误指在受影响实体内存上执行操作时，因缺少正确的边界数据验证，导致在其向关联的其他内存位置上执行了错误的读写操作，如缓冲区溢出、堆溢出等。

5.3.2.3.3 注入

5.3.2.3.3.1 概述

注入漏洞指受影响实体在通过用户输入构造命令、数据结构或记录的操作过程中，由于缺乏对用户输入数据的正确验证，导致未过滤或未正确过滤掉其中的特殊元素，引发的解析或解释方式错误问题。

5.3.2.3.3.2 格式化字符串错误

格式化字符串错误漏洞指受影响实体接收外部格式化字符串作为参数时，因参数类型、个数过滤不严格，导致的越界访问问题。

5.3.2.3.3.3 跨站脚本

跨站脚本漏洞指因缺少对客户端数据的正确验证，导致向其他客户端提供了错误的执行代码的问题。

5.3.2.3.3.4 命令注入

命令注入漏洞指受影响实体在构造可执行命令过程中，因未正确过滤其中的特殊元素，导致生成了错误的可执行命令。主要包括以下两类。

a) 操作系统命令注入漏洞：指受影响实体在构造操作系统可执行命令过程中，因未正确过滤其中的特殊字符等，导致生成了错误的操作系统执行命令。
b) 参数注入漏洞：指受影响实体在构造命令参数过程中，因未正确过滤参数中的特殊字符，导致生成了错误的执行命令。

5.3.2.3.3.5 代码注入

代码注入漏洞指受影响实体在通过外部输入数据构造代码段的过程中，因未正确过滤其中的特殊元素，导致生成了错误的代码段，修改了受影响实体的预期的执行控制流。

5.3.2.3.3.6 SQL 注入

SQL注入漏洞指受影响实体在基于数据库的应用中，因缺少对构成SQL语句的外部输入数据的验证，导致生成并执行了错误的SQL语句。

5.3.2.3.4 路径遍历

路径遍历漏洞指受影响实体因未能正确地过滤资源或文件路径中的特殊元素，导致访问受限目录之外的位置。

5.3.2.3.5 后置链接

后置链接漏洞指受影响实体在使用文件名访问文件时，因未正确过滤表示非预期资源的链接或者快捷方式的文件名，导致访问了错误的文件路径。

5.3.2.3.6 跨站请求伪造

跨站请求伪造漏洞是指受影响实体在WEB应用中，因未充分验证有效的请求是否来自可信用户，导致受欺骗的客户端向服务器发送非预期的请求。

5.3.2.4 数字错误

数字错误漏洞指受影响实体因未正确计算或转换所产生的的数字，导致的整数溢出、符号错误等问题。

5.3.2.5 竞争条件问题

竞争条件问题漏洞指受影响实体因在并发运行环境中，一段并发代码需要互斥地访问共享资源时，因另一段代码在同一个时间窗口可以并发修改共享资源而导致的安全问题。

5.3.2.6 处理逻辑错误

处理逻辑错误漏洞是受影响实体在设计实现过程中，因处理逻辑实现问题或分支覆盖不全面等原因造成的漏洞。

5.3.2.7 加密问题

加密问题漏洞指受影响实体未正确使用相关密码算法，导致的内容未正确加密、弱加密、明文存储敏感信息等问题。

5.3.2.8 授权问题

5.3.2.8.1 概述

授权问题漏洞指受影响实体因缺少身份验证措施或身份验证强度不足而导致的安全问题。

5.3.2.8.2 信任管理问题

信任管理问题漏洞指因缺乏有效的信任管理机制，导致受影响实体存在可被攻击者利用的默认密码或者硬编码密码、硬编码证书等问题。

5.3.2.8.3 权限许可和访问控制问题

权限许可和访问控制问题漏洞指受影响实体因缺乏有效的权限许可和访问控制措施而导致的安全问题。

5.3.2.9 数据转换问题

数据转换问题漏洞指受影响实体处理上下文因对数据类型、编码、格式、含义等理解不一致导致的安全问题。

5.3.2.10 未声明功能

未声明功能漏洞指受影响实体通过测试接口、调试接口等可执行非授权功能导致的安全问题。例如，若测试命令或调试命令在使用阶段仍可用，则可被攻击者用于显示存储器内容或执行其他功能。

5.3.3 配置错误

5.3.3.1 默认配置问题

配置错误漏洞指受影响实体在使用过程中因配置文件、配置参数或因默认不安全的配置状态而产生的漏洞。

5.3.3.2 弱口令

弱口令漏洞指受影响实体存在容易被别人猜测到或被破解工具破解的口令，多为简单的数字组合、账号相同的数字组合、键盘上的临近键或常见姓名。受影响实体出厂配置的默认密码等不属于弱口令范畴。

5.3.4 环境问题

5.3.4.1 概述

环境问题漏洞指因受影响实体部署运行环境的原因导致的安全问题。

5.3.4.2 信息泄露

5.3.4.2.1 概述

信息泄露漏洞指在运行过程中，因配置等错误导致的受影响实体信息被非授权获取的漏洞。

5.3.4.2.2 日志信息泄漏

日志信息泄漏漏洞指受影响实体因日志文件非正常输出导致的信息泄露。

5.3.4.2.3 调试信息泄漏

调试信息泄漏漏洞指受影响实体在运行过程中因调试信息输出导致的信息泄露。

5.3.4.2.4 侧信道信息泄露

侧信道信息泄露漏洞指受影响实体因功耗、电磁辐射、I/O特性、运算频率、时耗等侧信道信息的变化导致的信息泄露。

5.3.4.3 故障注入

故障注入漏洞指通过改变运行环境（如温度、电压、频率等，或通过注入强光等方式）触发，可能导致受影响实体代码、系统数据或执行过程发生错误的安全问题。

5.3.5 拒绝服务

拒绝服务漏洞指受影响实体因设计或实现不当，导致网络/系统资源耗尽，或服务暂时中断/停止，导致其正常用户无法访问。

5.3.6 其他

其他漏洞指暂时无法将漏洞归入上述任何类别，或者没有足够充分的信息对其进行分类，漏洞细节未指明的漏洞。

6 工业信息安全漏洞分级

6.1 概述

根据工业信息安全漏洞分级的目的不同，分为通用分级和现场分级两种分级方式，每种分级方式均分为超危、高危、中危和低危四个等级。其中通用分级为工业信息安全人员从技术角度对受影响实体的漏洞危害等级进行评估。现场分级为工业信息安全人员在特定场景、特定用途下，对漏洞危害等级进行评估。

6.2 工业信息安全漏洞分级指标

6.2.1 基础指标

6.2.1.1 可利用性指标

6.2.1.1.1 概述

可利用性指标反映了受影响实体的特征，具体包括访问路径、触发要求、权限需求、交互条件四个指标。每个可利用性指标都是针对受影响实体进行评分，并反映导致攻击成功的漏洞属性。可利用性分级见附录A。

6.2.1.1.2 访问路径

访问路径指触发漏洞的路径前提，反映漏洞触发时与受影响实体最低接触程度。

访问路径的赋值包括：网络、邻接、本地和物理。通常因网络、邻接、本地和物理触发的漏洞，其被利用性程度由高到低依次降序，访问路径赋值说明见表1。

表1 访问路径赋值说明

赋值	描述
网络	工业信息安全漏洞可以通过网络远程触发。
邻接	工业信息安全漏洞需通过共享的物理网络或逻辑网络触发。
本地	工业信息安全漏洞需要在本地环境中触发。
物理	工业信息安全漏洞需通过物理接触 / 操作才能触发。

6.2.1.1.3 触发要求

触发要求指漏洞成功触发的要求，反映受影响实体在系统环境的版本、配置、协议等因素影响下，成功触发漏洞的要求。

触发要求的赋值包括：低、高。通常触发要求低的漏洞危害程度高，触发要求赋值说明见表2。

表2 触发要求赋值说明

赋值	描述
低	工业信息漏洞触发对受影响实体的协议规范、配置参数、运行环境、版本等无特别要求，例如：默认的配置参数、普遍的运行环境、通用的协议规范等。
高	工业信息漏洞触发对受影响实体的配置参数、运行环境等有特别要求，例如：不常用的参数配置、特殊的运行环境条件、私有或不常用的协议等。

6.2.1.1.4 权限需求

权限需求指触发漏洞所需的权限，反映漏洞成功触发需要的最低的权限。

权限需求的赋值包括：无、低和高。通常所需要的权限越少漏洞危害程度越高，权限需求赋值说明见表3。

表3 权限需求赋值说明

赋值	描述
无	工业信息安全漏洞触发无需特殊的权限，只需要公开权限和匿名访问权限。
低	工业信息安全漏洞触发需要较低的权限，需要普通用户权限。
高	工业信息安全漏洞触发需要较高的权限，需要管理员权限。

6.2.1.1.5 交互条件

交互条件指漏洞触发是否需要其他主体（如：系统用户、外部用户、其他系统等）的参与、配合，反映漏洞触发时，是否需要除触发漏洞的主体之外的其他主体参与。

交互条件的赋值包括：不需要、需要。通常不需交互条件即能触发的漏洞，其危害程度较高，交互条件赋值说明见表4。

表4 交互条件赋值说明

赋值	描述
不需要	工业信息安全漏洞触发无需用户或系统的参与或配合。
需要	工业信息安全漏洞触发需要用户或系统的参与或配合。例如：通常跨站脚本漏洞、跨站请求伪造漏洞等需要用户的参与。

6.2.1.2 影响程度指标

6.2.1.2.1 概述

影响程度指标描述工业信息安全漏洞被成功利用所造成的危害及影响，包括最严重的直接或间接结果。影响程度指标包括物理影响、保密性影响、完整性影响和可用性影响四个指标。影响程度分级表见附录B。

6.2.1.2.2 物理影响

物理影响程度反映受影响实体与物理世界的交互、影响程度。物理影响程度的赋值包括：高、低，物理影响程度赋值说明见表5。

表5　物理影响赋值说明

赋值	描述
高	受影响实体的行为直接影响物理世界，例如：受影响实体可感知物理某实体的温度、流速等状态或执行操作以改变物理实体或环境的状态。
低	受影响实体的行为对物理世界的影响较小或无影响。

6.2.1.2.3　保密性影响

保密性影响指标反映漏洞对受影响实体承载（如：处理、存储、传输等）信息的保密性的影响程度。影响赋值为：严重、一般和无，保密性影响赋值说明见表6。

表6　保密性影响赋值说明

赋值	描述
严重	信息保密性影响严重，例如：保密性完全丢失，导致受影响实体的所有信息资源暴露给攻击者；或者攻击者只能得到一些受限信息，但被暴露的信息可以直接导致严重的信息丢失。
一般	信息保密性影响一般，例如：保密性部分丢失，攻击者可以获取一些受限信息，但是攻击者不能控制获得信息的数量和种类。被暴露的信息不会引起受影响实体直接的、严重的信息丢失。
无	信息保密性无影响，漏洞对保密性不产生影响。

6.2.1.2.4　完整性影响

完整性影响指标反映漏洞对受影响实体承载（如：处理、存储、传输等）信息的完整性的影响程度。影响赋值为：严重、一般和无，完整性影响赋值说明见表7。

表7　完整性影响赋值说明

赋值	描述
严重	信息完整性破坏严重，例如：完整性完全丢失，攻击者能够修改受影响实体中的任何信息；或者，攻击者只能修改一些信息，但是，能够对受影响实体带来严重的后果。
一般	信息完整性破坏程度一般，例如：完整性部分丢失，攻击者可以修改信息，信息修改不会给受影响实体带来严重的影响。
无	信息完整性无影响，漏洞对完整性不产生影响。

6.2.1.2.5　可用性影响

可用性影响指标反映漏洞对受影响实体承载（如：处理、存储、传输等）信息的可用性的影响程度。影响赋值为：严重、一般和无，可用性影响赋值说明见表8。

表8　可用性影响赋值说明

赋值	描述
严重	信息可用性破坏严重。可用性完全丧失，攻击者能够完全破坏对受影响实体中信息资源的使用访问；或者，攻击者可破坏部分信息的可用性，但是能够给受影响实体带来直接严重的后果。
一般	信息可用性破坏程度一般。可用性部分丧失，攻击者能够降低信息资源的性能或者导致其可用性降低。受影响实体的资源是部分可用的，或在某些情况是完全可用的，但总体上不会给受影响实体带来直接严重的后果。
无	信息可用性无影响，漏洞对可用性不产生影响。

6.2.2　辅助因素指标

6.2.2.1　概述

辅助因素指标衡量当前漏洞可利用难度，是否存在任何补丁或解决方法，受影响实体在国内的分布情况。辅助因数分级表见附录C。

6.2.2.2 可利用难度

可利用难度包括：低、中、高。通常难度越低，漏洞的危害越严重，可利用难度赋值说明见表9。

可利用难度指标反映在参考环境下（例如：当前全球互联网环境，或者某企业内网环境等），漏洞触发所需的成本，例如：是否有公开的漏洞触发工具、漏洞触发需要的设备是否容易获取等。

表9 可利用难度赋值说明

赋值	描述
低	漏洞触发所需资源很容易获取，成本低，通常付出很少的成本即可成功触发漏洞，例如：漏洞触发工具已被公开下载、受影响实体暴露在公开网络环境下等。
中	漏洞触发所需的部分资源比较容易获取，成本不高，在现有条件基础上通过一定的技术、资源投入可以触发漏洞，例如：漏洞触发原理已公开但是无相应工具、漏洞触发需要某种硬件设备、漏洞触发需要一定的网络资源等。
高	漏洞触发需要的资源多，成本高，难于获取，例如：漏洞脆弱性组件未暴露在公开网络、漏洞触发工具难以获取等。

6.2.2.3 修补难度

修补难度包括：高、中、低。通常漏洞修补的难度越高，危害越严重，修补难度赋值说明见表10。

修补难度指标反映在参考环境下（例如：当前全球互联网环境，或者某企业内网环境等），修复漏洞所需的成本。

表10 修补难度赋值说明

赋值	描述
高	缺少有效、可行的修补方案，或者修补方案难以执行，例如：无法获取相应的漏洞补丁、由于某种原因无法安装补丁、无有效的修补措施等。
中	虽然有修补方案，但是需要付出一定的成本，或者修复方案可能影响系统的使用，或者修复方案非常复杂，适用性差，例如：虽然有补丁或漏洞修补措施，但是需要关闭某些网络服务等。
低	已有完善的修补方案，例如：已有相应漏洞的补丁或有效可行的修补措施等。

6.2.2.4 影响范围

影响范围包括：高、中、低、无。通常受影响实体在全国的分布更广泛，危害越严重，影响范围赋值说明见表11。影响范围指标反映受影响实体在全国范围的分布情况，包括受影响实体种类个数、涉及省市（自治区、直辖市），全国受影响实体数量等方面。

表11 影响范围赋值说明

赋值	描述
高	受影响实体众多，在全国范围内分布广泛且用户量庞大。
中	受影响实体在全国范围内分布较为广泛或集中在重要城市，或具有一定程度的用户量。
低	受影响实体在全国范围内分布稀疏，或用户量较少。
无	受影响实体单一，基本在全国范围内无分布，用户稀少。

6.2.3 环境因素指标

环境因素指标衡量受影响实体在现实环境中的使用范围及重要性，包括修复的时间代价、资产代价，受影响实体所含数据的数据量及敏感程度。环境因素分级表见附录D。

6.2.3.1 修复时间代价

修复时间代价指标反映实际现场修补漏洞所需的时间代价，如只能在特定时间更新、修复后需多长时间方才进入正常运行状态。修复时间代价赋值为：严重、一般和无，修复时间代价赋值说明见表12。

表12 修复时间代价赋值说明

赋值	描述
严重	漏洞修补所需的整体时间周期长。例如只能在特定时间进行修补，或修补过程消耗时间长，或修补后需长时间方可恢复至正常状态。
一般	漏洞修补所需的整体时间周期一般。例如修补过程消耗时间适中，或修补后恢复至正常状态的时间可接受。
无	漏洞修补及恢复正常状态的时间较短或基本可忽略。

6.2.3.2 修复资产代价

修复资产代价指标反映实际现场修补漏洞所需的资产代价，如修补过程需更换贵重实体（如：系统、模块、软硬件等）情况、恢复正常运行状态需造成的经济损失等。修复资产代价赋值为：严重、一般和无，修复资产代价赋值说明见表13。

表13 修复资产代价赋值说明

赋值	描述
严重	漏洞修补所产生的资产损失严重。例如修补时需更换多个贵重实体，或恢复至正常状态过程中造成严重的经济损失。
一般	漏洞修补所产生的资产损失一般。例如修补时需更换少量贵重实体，或恢复至正常状态过程中的经济损失一般。
无	漏洞修补及恢复正常状态过程中的经济损失微小或基本可忽略。

6.2.3.3 修复急迫性

修复急迫性指标反映该漏洞触发对实际现场的影响，修复急迫性赋值为：严重、一般和无，通常漏洞对环境的影响越高，危害越严重，修复急迫性赋值说明见表14。

表14 修复急迫性赋值说明

赋值	描述
严重	无有效的安全防护措施且触发漏洞会对系统、资产等造成严重影响，具有较高的修补优先级。
一般	具有一定的安全防护措施，触发漏洞会对系统、资产等造成中等程度的影响，修补优先级一般。
无	具有较强的安全防护措施，触发漏洞只会对系统、资产等造成轻微的影响，可暂缓修补或不修补。

6.2.3.4 数据敏感性

数据敏感性指标反映受影响实体所含数据的敏感程度，数据敏感性赋值为：严重、一般和无，通常受影响实体存储的数据敏感性越高，危害越严重，数据敏感性赋值说明见表15。

表15 数据敏感性赋值说明

赋值	描述
严重	受影响实体包含大量的敏感信息，其信息损坏将造成严重后果。
一般	受影响实体包含一定数量的敏感信息，其信息损坏将造成一定程度的后果。
无	受影响实体包含稀少的敏感信息，其信息损坏造成后果忽略不计。

6.3 工业信息安全漏洞分级方法

工业信息安全漏洞分级过程主要包括最初的指标赋值、指标分级、最终分级三个步骤，指标赋值是根据具体漏洞信息对其各类指标进行人工赋值；指标分级是根据指标赋值结果计算产生分级结果；最终分级是将指标分级计算生成通用分级和现场分级的结果，其中通用分级是选取基础指标、辅助因素指标两类指标计算产生，现场分级由基础指标、辅助因素指标和环境因素指标三类指标计算产生。漏洞分级过程见图2。

工业信息安全漏洞通用分级和现场分级均分为超危、高危、中危和低危四个等级，见附录E和附录F，具体内容如下：

a） 超危：工业信息安全漏洞可以非常容易地对受影响实体以及其关联的物理世界（国家、社会秩序、公共利益、人员安全、生产流程等）造成特别严重后果。

b） 高危：工业信息安全漏洞可以容易地对受影响实体以及其关联的物理世界（国家、社会秩序、公共利益、人员安全、生产流程等）造成严重后果。

c） 中危：工业信息安全漏洞可以对受影响实体造成一般后果，或者比较困难地对受影响实体以及其关联的物理世界（国家、社会秩序、公共利益、人员安全、生产流程等）造成严重后果。

d） 低危：工业信息安全漏洞可以对受影响实体以及其关联的物理世界（国家、社会秩序、公共利益、人员安全、生产流程等）造成轻微后果，或者比较困难地对受影响实体以及其关联的物理世界造成一般严重后果，或者非常困难地对受影响实体以及其关联的物理世界造成严重后果。

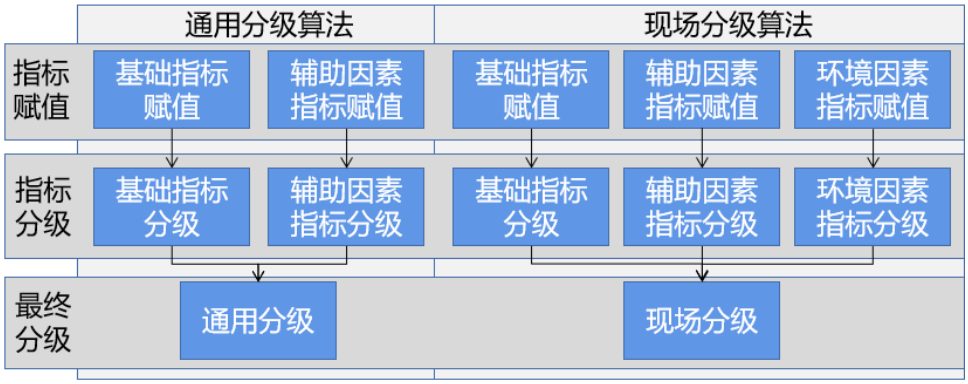

图2　漏洞分级过程示意图

附 录 A
（资料性）
可利用性分级表

可利用性分级见表A.1。

表A.1 可利用性分级

序号	访问路径	触发要求	权限需求	交互条件	可利用性分级
1	网络	低	无	不需要	9
2	网络	低	低	不需要	8
3	网络	低	无	需要	
4	邻接	低	无	不需要	
5	本地	低	无	不需要	
6	网络	高	无	不需要	
7	网络	低	低	需要	7
8	邻接	低	低	不需要	
9	网络	低	高	不需要	
10	邻接	低	无	需要	6
11	本地	低	无	需要	
12	本地	低	低	不需要	
13	网络	高	低	不需要	5
14	网络	高	无	需要	
15	邻接	高	无	不需要	
16	邻接	低	低	需要	
17	邻接	高	无	需要	4
18	邻接	高	低	不需要	
19	本地	高	无	不需要	
20	本地	低	低	需要	
21	网络	高	低	需要	
22	本地	高	低	不需要	3
23	网络	高	高	不需要	
24	网络	低	高	需要	
25	邻接	低	高	需要	
26	邻接	低	高	不需要	
27	本地	低	高	不需要	2
28	本地	高	无	需要	
29	物理	低	无	不需要	
30	网络	高	高	需要	
31	邻接	高	高	不需要	
32	邻接	高	低	需要	
33	本地	低	高	需要	
34	物理	低	无	需要	
35	物理	低	低	不需要	
36	本地	高	高	不需要	
37	本地	高	低	需要	1
38	邻接	高	高	需要	
39	物理	高	无	不需要	
40	物理	低	高	不需要	
41	物理	低	低	需要	
42	物理	高	低	不需要	
43	本地	高	高	需要	
44	物理	高	无	需要	

序号	访问路径	触发要求	权限需求	交互条件	可利用性分级
45	物理	高	高	需要	
46	物理	高	高	不需要	
47	物理	高	低	需要	
48	物理	低	高	需要	
注：按照“访问路径”“触发要求”“权限需求”“交互条件”的不同，可分为48种组合情况，按照每种组合的可利用程度的差异，从高到低可分为9个级别。					

附 录 B
（资料性）
影响程度分级表

影响程度分级见表B.1。

表B.1 影响程度分级

序号	物理影响	保密性	完整性	可用性	影响程度分级
1	低	严重	严重	严重	9
2		严重	严重	一般	8
3		严重	一般	严重	8
4		一般	严重	严重	8
5		严重	严重	无	7
6		严重	无	严重	7
7		无	严重	严重	7
8		严重	一般	一般	6
9		一般	一般	严重	6
10		一般	严重	一般	6
11		严重	一般	无	5
12		严重	无	一般	5
13		一般	严重	无	5
14		一般	无	严重	5
15		无	严重	一般	5
16		无	一般	严重	5
17		严重	无	无	4
18		无	严重	无	4
19		无	无	严重	4
20		一般	一般	一般	3
21		一般	一般	无	2
22		一般	无	一般	2
23		无	一般	一般	2
24		一般	无	无	1
25		无	一般	无	1
26		一般	一般	无	1
27	高	严重	严重	严重	9
28		严重	严重	一般	8
29		严重	一般	严重	8
30		严重	严重	无	8
31		严重	无	严重	8
32		严重	一般	一般	7
33		严重	一般	无	7
34		严重	无	一般	7
35		严重	无	无	7
36		一般	一般	严重	6
37		一般	严重	一般	6
38		一般	严重	严重	6
39		一般	严重	无	6
40		一般	无	严重	6
41		一般	一般	一般	5
42		一般	一般	无	5
43		一般	无	一般	5
44		一般	无	无	4

序号	物理影响	保密性	完整性	可用性	影响程度分级
45		无	严重	严重	3
46		无	严重	一般	3
47		无	一般	严重	3
48		无	严重	无	3
49		无	无	严重	3
50		无	一般	一般	2
51		无	一般	无	1
52		无	无	一般	1
53		无	无	无	1

附 录 C
（资料性）
辅助因素分级表

辅助因素分级见表C.1。

表C.1 辅助因素分级

序号	可利用难度	修补难度	影响范围	辅助因素分级
1	低	高	高	9
2	中	高	高	8
3	低	中	高	8
4	低	高	中	8
5	低	中	中	7
6	低	高	低	7
7	低	低	高	7
8	高	高	高	7
9	中	中	高	7
10	中	高	中	7
11	高	高	中	6
12	高	中	高	6
13	低	中	低	6
14	低	低	中	6
15	中	中	中	6
16	高	高	低	5
17	高	低	高	5
18	高	中	中	5
19	中	低	中	5
20	中	中	低	5
21	高	中	低	4
22	高	低	中	4
23	中	低	高	4
24	中	高	低	4
25	低	低	低	3
26	中	低	低	2
27	高	低	低	1
注：按照“可利用难度”“修补难度”“影响范围”的不同，可分为27种组合情况，按照每种辅助因素组合的差异，从高到低可分为9个等级。				

附 录 D
（资料性）
环境因素分级表

环境因素分级见表D.1。

表 D.1 环境因素分级

序号	严重（次数）	一般（次数）	无（次数）	环境因素分级
1	4	0	0	9
2	3	1	0	8
3	3	0	1	8
4	2	2	0	7
5	2	1	1	7
6	2	0	2	6
7	1	3	0	6
8	1	1	2	5
9	1	2	1	5
10	1	0	3	4
11	0	4	0	4
12	0	3	1	3
13	0	2	2	3
14	0	1	3	2
15	0	0	4	1
注：修复时间代价、修复资产代价、修复急迫性、数据敏感性权重相同，按照环境因素指标“严重”“一般”“无”的数量进行环境因素的分级。				

附 录 E
（资料性）
漏洞通用分级表

漏洞通用分级见表E.1。

表 E.1 漏洞通用分级

序号	可利用性分级	影响程度分级	辅助因素分级	通用分级
1	8-9	8-9	8-9	超危
2	8-9	7	7	高危
3	8-9	1-9	4-6	高危
4	5-7	7-9	7-9	高危
5	8-9	7-9	1-3	中危
6	8-9	1-6	1-6	中危
7	5-7	7-9	1-6	中危
8	5-7	1-6	1-9	中危
9	3-4	4-9	1-9	中危
10	3-4	1-3	3-9	中危
11	1-2	7-9	1-9	中危
12	1-2	4-6	3-9	中危
13	3-4	1-3	1-2	低危
14	1-2	4-6	1-2	低危
15	1-2	1-3	1-9	低危

附 录 F
（资料性）
漏洞现场分级表

漏洞现场分级见表F.1。

表 F.1 漏洞现场分级

序号	通用分级	环境因素	现场分级
1	超危	7-9	超危
2	超危	4-6	高危
3	超危	1-3	中危
4	高危	8-9	超危
5	高危	7	高危
6	高危	4-6	中危
7	高危	1-3	低危
8	中危	9	超危
9	中危	7-8	高危
10	中危	4-6	中危
11	中危	1-3	低危
12	低危	7-9	高危
13	低危	4-6	中危
14	低危	1-3	低危

参 考 文 献

[1] GB/T 30276-2020 信息安全技术 网络安全漏洞管理规范
[2] GB/T 37954-2019 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法
[3] 工业互联网企业网络安全分类分级指南（试行）