ICS 国际标准分类号
CCS 中国标准文献分类号

团　　体　　标　　准

T/CES XXX-XXXX

电力系统网络安全风险评价与防御导则

Guide rule of risk assessment and defense for power system network security vulnerabilities

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电工技术学会　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》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。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会能源智慧化标准工作组归口。

本文件起草单位：国网山西省电力公司电力科学研究院、国网信息通信产业集团有限公司、四川中电启明星有限公司、华北电力大学、安徽继远检验检测技术有限公司、南京南瑞信息通信科技有限公司、北京中电普华信息技术有限公司。

本文件主要起草人：芦山、付昀夕、刘泽辉、王振亚、杨华、杨姝、周自强、马东娟、刘泽三、宫晓辉、凌浩洁、张文娟、闫晨阳、张敏、高紫婷、闫廷廷、黄元、李杉、李廷顺、靳鑫、潘安顺、富思、沈耀威、任彦斌、宋亚琼、王军、韩泽华、苑学贺、董爱强、刘振圻、南淑君。

本文件为首次发布。

电力系统网络安全风险评价与防御导则

1 范围

本标准规定了电力系统中网络安全漏洞的种类、分级以及管理措施。它旨在通过全面分析网络安全漏洞，增强电力系统的稳定性和可靠性。本标准提供了一个安全漏洞管理框架，旨在通过识别、评估和应对安全漏洞，持续监控和改进电力系统的网络安全。

本标准适用于电力系统网络安全管理的硬件、软件和网络通信等多个层面，给出了各类漏洞分类方法、评级标准以及相应的防御策略。

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 28458-2012 信息安全技术 安全漏洞标识与描述规范

GB/T 30276-2013 信息安全技术 信息安全漏洞管理规范

GB/T 33561-2017 信息安全技术安全漏洞分类.

GB/T 36572-2018 电力监控系统网络安全防护导则

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全漏洞 Network Security Vulnerability

网络安全漏洞是指存在于各类信息系统的网络组件、软件或硬件中的设计或实施缺陷。这些缺陷广泛存在于各行各业的信息技术基础设施中，当这些缺陷被恶意行为者发现并利用时，可能威胁到相关系统的安全性、稳定性及数据的保密性、完整性和可用性。

[来源：GB/T 30279-2020 信息安全技术安全漏洞等级划分指南,5.1]

3.2

电力系统网络 Power System Network

涵盖所有电力传输和分配网络元件的信息和通信技术基础设施，包括用于管理、监控和保护电力系统运行的软件和硬件工具。

[来源：GB/T 36572-2018 电力监控系统网络安全防护导则,3 术语和定义]

3.3

风险评估 Risk Assessment

一个系统性的过程，用于识别安全威胁和漏洞，并评估这些威胁和漏洞如果被利用所可能造成的损害程度，以及发生的可能性。

[来源：GB/T 30279-2020 信息安全技术安全漏洞等级划分指南,5.1]

3.4

漏洞利用 Vulnerability Exploitation

通过技术手段利用已识别的安全漏洞来入侵或造成电力系统网络的破坏。

[来源：GB/T 30279-2020 信息安全技术安全漏洞等级划分指南,5.1]

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

api：应用程序接口（application programming interface）

des：数据加密标准（data encryption standard）

ids：入侵检测系统（intrusion detection system）

ips：入侵防御系统（intrusion prevention system）

sql：结构化查询语言（structured query language）

xss：跨站脚本（cross-site scripting）

5 网络安全漏洞分类

5.1 根据漏洞来源

5.1.1 软件漏洞

软件漏洞是电力系统网络中常见的安全威胁，这些漏洞主要源于内部程序的缺陷。具体可以细化为以下两类：

a）设计缺陷：设计缺陷通常在软件的规划和设计阶段形成，源于需求分析不充分或安全性设计被忽略。特别是在电力控制系统中，若未充分考虑数据加密或用户身份验证机制，可能导致认证被绕过、权限被不当提升，或关键操作数据泄漏。例如，如果一个电力监控系统设计时未加入足够的用户访问级别控制，可能允许低级别用户访问本应受限的操作界面或数据，从而增加系统被滥用或攻击的风险。

b）编程错误：编程错误是在软件开发过程中引入的漏洞，包括缓冲区溢出、输入验证不当、以及逻辑错误等。这些漏洞常因开发人员不熟悉或忽视电力系统的安全编码标准和最佳实践而发生。在电力系统中，这些编程失误可能允许攻击者执行未授权代码、访问或修改智能电表读数，甚至操控电网设备或窃取敏感信息。例如，如果电力系统的应用程序未正确处理用户输入，可能导致 SQL 注入攻击，攻击者可以利用这一点访问或篡改储存的电网运行数据。

5.1.2 硬件漏洞

硬件漏洞涉及到电力系统中使用的物理设备，这些漏洞可能由物理损坏、设计缺陷或生产过程中的错误造成。

a）物理缺陷：物理缺陷指的是电力设备因材料疲劳、自然老化或外部物理冲击导致的功能故障或性能下降。例如，变压器可能因长期运行而导致其冷却系统效率降低，若未及时维护和替换，可能引起过热甚至火灾，从而威胁到整个电力系统的稳定性和安全性。这种类型的缺陷通常需要通过定期检查和维护来管理和预防。

b）制造缺陷：制造缺陷通常源于电力设备生产过程中的质量控制失败，如高压断路器的机械部件可能因制造不良而无法正常操作。例如，电力电缆可能因为使用了不符合标准的绝缘材料而在运行中出现绝缘层破损，导致短路或电击事故。这些问题可能在设备投入运行初期不被发现，但一旦出现，其后果往往严重，如导致电力系统的部分或完全停运。解决这类问题需要从源头加强生产过程的质量监控和成品检验。

5.1.3 配置漏洞

配置漏洞通常是由于电力设备或软件配置不当导致的安全风险。

a）错误配置：错误配置涉及到不当的系统设置或参数配置。这些配置错误可能为攻击者提供进入系统的途径。例如，一个电力控制系统中的防火墙规则若设置不当，可能允许未授权的访问，或是一个关键的安全协议如 SSH 如果配置了弱或默认密码，都可能使系统容易受到攻击。针对此类问题，有效的应对措施包括定期进行配置审计，确保所有系统配置符合安全最佳实践。

b）默认配置：许多电力系统组件和控制软件在出厂时都设有默认配置，这些设置通常为了用户便利而非最大化安全性。如果这些默认配置未被更改，它们可能成为攻击的切入点。例如，网络设备或管理界面可能默认启用简单的用户名和密码，如果未进行更改，这些默认设置可被利用作为攻击的切入点。为防止此类安全风险，重要的是在设备初次安装或软件首次运行时，立即更改所有默认密码和配置，并关闭不必要的服务。

5.2 按位置分类

5.2.1 协同层

协同层漏洞出现在跨电力系统或多应用间的协作接口或服务中。这类漏洞主要由接口集成不当造成，如数据交换格式不一致或认证机制不兼容，这可能导致数据在传输过程中的泄漏、篡改或丢失。具体包括 API 安全漏洞，允许未授权的第三方应用访问或修改敏感数据，以及身份验证绕过，导致未经授权的系统访问。

5.2.2 应用层

应用层漏洞直接关联到电力系统中使用的软件应用，涵盖 web 应用、数据库和其他应用软件。这些漏洞包括输入验证不足，可能导致 SQL 注入或跨站脚本攻击，会话管理缺陷可能使攻击者劫持用户会话。这类漏洞主要由软件设计不当或编码错误造成。

5.2.3 网络层

网络层漏洞涉及数据传输和通信协议，存在于数据包的路由和转发过程中。常见漏洞包括服务拒绝攻击、IP 欺骗、以及路由劫持等，这些漏洞通常源于网络协议的安全缺陷或网络设备配置不当。在电力系统中，此类漏洞可能导致关键操作数据的丢失或篡改，影响电力调度和配电的准确性。

5.2.4 系统层

系统层漏洞存在于电力操作系统或系统服务的核心组件中，可能导致权限提升、未授权访问或系统资源的滥用。这些漏洞往往是由于操作系统本身的安全缺陷或配置错误引起的。防御措施包括定期更新操作系统和软件以修复已知漏洞，定期进行风险评估，实施最小权限原则以限制系统资源的访问，以及监控系统活动以侦测异常行为，从而提升电力系统的系统层安全性，保护关键基础设施免受攻击。

5.2.5 硬件层

硬件层漏洞源自电力设备的安全弱点，包括但不限于服务器、网络设备及其他支持设备。这些问题可能包括固件中的后门、硬件设计缺陷或物理接口安全缺陷，通常由设备制造过程中的质量控制失败或设计不足引起。硬件层的漏洞可能直接影响到电力控制系统的稳定运行和数据安全。因此，防御措施应包括严格的供应链管理，确保从可靠的供应商采购设备，并对进入电力系统的所有硬件设备进行严格的安全审查。

5.2.6 数据处理层

数据处理层漏洞涉及到在电力系统网络中对收集到的数据进行存储、处理和分析的软件系统。这包括数据管理和分析工具，如数据仓库、大数据分析平台等。这类漏洞通常源于软件编程错误或配置不当，如不安全的数据存储机制或缺乏有效的数据访问控制，可能导致敏感信息泄露或非法修改。常见的漏洞包括不当的数据访问权限配置、缺少数据加密措施或未经授权的数据访问等。

在数据处理层，为防止信息泄露和非法修改，应实行严格的安全编码和代码审查流程，加强基于角色的访问控制系统，并采用强加密措施保护数据的存储与传输。同时，建立定期的数据备份和快速有效的灾难恢复策略，以应对可能的数据丢失或损坏。

5.2.7 感知层

感知层漏洞主要发生在电力系统网络的物理设备和传感器上，这包括但不限于智能计量设备、环境监测装置及其他数据采集设备。这类漏洞可能由硬件设计缺陷、固件更新不及时或配置错误引起。具体表现为设备身份认证机制弱或缺失，使得攻击者能够伪装设备进行数据篡改或发起拒绝服务攻击。此外，数据采集过程中的加密措施不足，也可能导致数据在传输过程中被截获或篡改。

针对感知层的安全威胁，应增强物理设备的身份验证和完整性验证措施，包括采用多因素认证。同时，保持设备固件和软件的最新状态，及时应用安全更新和补丁。此外，对所有数据传输实施端到端加密，以确保数据在采集和传输过程中的安全性。

5.3 按技术类型分类

5.3.1 缓冲区溢出

a）当程序错误地向缓冲区写入超出其容量的数据时，就会缓冲区溢出漏洞，允许攻击者执行任意代码或破坏内存布局。这可能导致对电力控制系统的非法控制或服务拒绝攻击，威胁电网的稳定和安全。

b）为有效防止缓冲区溢出漏洞，电力系统的软件开发团队应定期进行源代码审查和静态代码分析，这有助于及早发现并修复潜在的缓冲区溢出风险。例如，使用工具如 Splint 或 Coverity 可以自动检测潜在的缓冲区溢出问题。其次，实施如堆栈保护机制（例如使用 Canary 值防护机制）和地址空间布局随机化等运行时保护技术。这些措施通过增加内存错误的不可预测性，提高了攻击者利用此类漏洞的难度。

5.3.2 SQL 注入

a）SQL 注入指的是攻击者通过将恶意 SQL 命令插入到应用程序预期执行的查询中，来操纵后端数据库。此类攻击可以用来绕过认证机制、窃取、修改或删除数据。电力系统中的数据管理系统如果处理不当，便可能遭受 SQL 注入，导致关键运营数据的泄露或损坏。例如，攻击者可能通过注入删除命令（如 DELETE FROM 语句）来删除电力数据，影响运营或导致错误的决策，从而严重影响电网的稳定性和安全性。

b）应用程序必须对所有用户输入进行严格的验证和清洗，确保输入数据不含有恶意 SQL 命令。使用参数化查询是一种有效的防御策略，如在编程时使用预备语句（Prepared Statements）而不是直接将用户输入拼接到 SQL 查询中。此外，对数据库的访问权限进行严格控制，确保每个用户或应用程序只拥有完成其任务所必需的最小权限。

5.3.3 跨站脚本

a）跨站脚本漏洞指的是利用网页应用在处理用户输入数据时的疏漏来执行恶意脚本。这种漏洞允许攻击者在用户的浏览器上运行恶意脚本，从而可能窃取 Cookies、会话令牌或其他敏感信息，甚至篡改网页内容。在电力系统中，跨站脚本攻击主要针对基于网页的管理控制界面或用户交互平台，这些界面通常用于监控和控制电网运行，因此，跨站脚本攻击可能导致电网操作指令被篡改或敏感信息的泄露。例如，攻击者可能注入脚本到电网监控系统的用户反馈表单中，当系统管理员查看反馈内容时，该脚本被触发并执行，导致管理员的会话令牌被窃取，从而使攻击者能够非法控制电网操作。

b）针对跨站脚本攻击的防护措施包括在用户输入和输出阶段实施严格的数据清洗和编码措施，确保所有输入数据在处理前被适当清洗和验证，防止恶意脚本的注入。同时，部署内容安全政策，该政策可以帮助限制网页可加载和执行的资源，有效隔离和防止不受信任的内容执行。例如，CSP 可以设定只允许从已知安全的源加载脚本，从而大大减少恶意脚本执行的机会。

5.3.4 加密相关安全漏洞

在电力系统中，加密技术是确保数据传输和存储过程中信息安全的关键。远程操作命令和敏感操作数据的加密保护至关重要，因为加密漏洞可能导致这些敏感信息被非法解密和利用，从而威胁到整个电力系统的安全与稳定。

a）加密算法缺陷：加密算法的缺陷通常涉及到算法设计本身的问题或者实现过程中的错误，这可以导致预期的安全性被削弱或完全失效。在电力系统的网络安全中，加密算法用于保护数据的完整性和保密性，特别是在数据传输和存储过程中。一个有缺陷的加密算法可能使得敏感信息如操作命令、监控数据和个人信息容易被解密。加密算法可能存在的问题包括使用已被证明为不安全的算法，或者在加密实现过程中引入的错误，如随机数生成器的弱点。这些问题可能被攻击者利用，通过密码分析技术破解加密措施，获取未授权的数据访问。

b）密钥管理问题：不当的密钥管理，包括密钥生成、存储、分发和销毁的过程中的缺陷，都可能导致安全风险，使得整个加密体系受到威胁。在电力系统中，密钥管理问题可能导致对控制系统的未授权访问或数据泄露。常见的密钥管理问题包括密钥泄露、使用硬编码密钥以及密钥更新和撤销流程的不足。

针对加密漏洞，电力网络系统应采用行业认可的强加密算法，并避免使用已知存在弱点的算法。建立全面的密钥管理政策，包括密钥的安全生成、存储、使用和废弃，确保密钥的完整性和保密性。定期对使用的加密技术进行安全审查和测试，确保加密措施能够抵抗最新的威胁和攻击方法。

5.3.5 命令注入

a）命令注入漏洞是一种严重的安全威胁，发生在攻击者能够在应用程序中注入未经授权的命令或代码，导致这些命令在电力系统的控制服务器上执行。这可能涉及到对电网控制系统的非法操作，包括修改供电调度逻辑或干预服务的正常运行等非法操作，进而可能导致电力供应中断或系统稳定性受损。

b）为抵御命令注入，应利用参数化的命令接口，并对所有外部输入进行严格的验证和清洗，确保输入不可被解释为控制命令。

5.3.6 API 安全

a）API（应用程序编程接口，Application Programming Interface）安全是指确保通过网络应用程序提供的接口免受未授权访问和攻击的措施。在电力系统中，API 常用于系统组件之间的数据交换、设备管理以及与远程控制系统的接口，是电力网络基础设施的关键组成部分。不安全的 API 可能导致敏感数据泄露、服务中断甚至系统控制权的丧失。例如，API 泄露的敏感数据可能包括消费者信息、操作日志或即时系统状态，这些信息的泄露可被用于进一步的攻击策划。

b）为确保 API 的安全性，必须实施综合的认证和授权措施，以验证访问者身份并严格限制其权限。对 API 调用实施速率限制，以防止滥用并减轻拒绝服务攻击的风险。同时，通过实时监控 API 的使用情况，可以快速发现并响应异常行为，防止安全漏洞被利用。

5.3.7 会话劫持

a）会话劫持漏洞发生在攻击者能够非法接管用户的会话控制之后，通常是通过预测或窃取会话令牌（Cookies 等）实现的。在电力系统的监控和控制网络中，会话劫持可能允许攻击者获取对敏感操作界面的未授权访问，进而控制或破坏电力设施。

b）防止会话劫持应采取的措施包括采用难以预测的会话令牌，使用仅通过安全渠道传输的 HttpOnly 和 Secure 属性的 Cookies，并确保整个会话通过 HTTPS 协议加密。

5.3.8 跨站请求伪造

a）跨站请求伪造攻击让攻击者能够在用户不知情的情况下，以该用户的身份执行恶意请求。这种类型的攻击对电力系统的网络安全尤为危险，因为它可能用于更改系统设置或发出具有破坏性的指令，如关闭电力供应。

b）防护跨站请求伪造的有效策略包括引入 CSRF 令牌机制，在每次提交请求时验证这些随机生成的令牌。此外，验证引用来源（Referer）头部信息和设置 Cookies 的 SameSite 属性可以进一步限制跨站请求的能力，从而减少未授权操作的风险。

5.3.9 目录遍历

a）目录遍历（或文件路径遍历）漏洞允许攻击者访问文件系统上，本不应允许访问的文件和目录。这种漏洞通常由于网站或应用程序未能适当地限制用户能够访问的文件路径。在电力系统中，这可能导致配置文件、数据库或其他敏感数据的泄漏。例如，攻击者可能利用目录遍历漏洞读取含有网络配置详情的文件，进一步攻击系统。

b）对抗目录遍历攻击，应通过严格的输入验证来禁止包含目录遍历序列的输入。使用安全的文件操作 API 并限制应用程序的文件系统访问权限至必需的最小范围，可以通过运行应用程序在最小权限用户账户下，或在操作系统级别设置文件和目录的访问权限，确保应用程序只能访问其执行必需任务所需的文件系统部分。

6 网络安全漏洞分级

6.1 漏洞利用难度分级

6.1.1 可获取性与公开程度

a） 未公开（利用难度系数：6）:这类漏洞未被公开披露，通常只有软件开发者、安全研究者或黑客中极小部分人知道。这类漏洞的存在可能由于负责披露的个人或组织选择保留信息，等待发布修补程序或直到正确的时间点来进行公开。

b） 限制性披露（利用难度系数：5）:这类漏洞的信息可能仅在特定的社区、论坛或者安全研究团体内部共享，可获取性较低。这种情况下，有限的公众得知漏洞，但仍未大范围公开。

c） 已知未利用（利用难度系数：4）：这类漏洞可能已经公开，但是由于缺乏自动化工具或者只有很少的影响案例，实际上它们还未被广泛利用。只在专业论坛或邮件列表上讨论，其技术详情并未广为人知。

d） 公开且已有利用（利用难度系数：3）：这类漏洞不仅已经完全公开，对其的深入分析及可能的利用代码也在互联网上轻松获取，如在安全社区网站、博客和公共漏洞数据库中。这些漏洞可能已经有相应的工具和脚本可供使用，攻击者可以较轻松地利用。

e） 有公开且易操作的攻击工具（利用难度系数：2）：这类漏洞不仅信息公开并且已被广泛利用，还伴有成熟、易用的攻击工具或脚本，允许攻击者即使没有深入的技术知识也能轻松开展攻击。这些工具可能集成在黑客工具包中，或者以自动化的脚本形式存在，甚至可能被并入商业化的渗透测试软件。

f） 流行和广泛利用（利用难度系数：1）：这类漏洞已经非常流行且被广泛用于恶意软件、勒索软件或其他大规模网络攻击活动。通常，对这些漏洞的利用及其攻击模式的细节通过安全广播和媒体报道得到大量公开。

6.1.2 利用条件限制分类

a） 无条件限制

1） 描述：漏洞可以通过网络远程利用，不需要任何用户互动，也不依赖特定的系统配置或状态。攻击者不需要任何特权即可发起攻击。

2） 示例：远程执行代码漏洞允许攻击者通过发送恶意制作的数据包到目标应用程序（不需要认证）来远程控制目标系统。

b） 最低限制

1） 描述：攻击可以远程启动，但可能需要一些基本的条件。

2） 示例：社会工程攻击，诸如点击一个看似无害但实际上包含恶意载荷的电子邮件链接导致中毒。

c） 中等限制

1） 描述：漏洞可以远程利用，但需要较多的条件，可能需攻击者拥有部分系统信息，如特定的用户输入或猜测凭证。

2） 示例：对网络应用程序进行的跨站请求伪造攻击，需要受害者在持有会话的同时，点击或提交一个特制的表单。

d） 高限制

1） 描述：要求攻击者已经有了对受害系统内部网络的访问，或者需要启用了特殊设置和特定版本的软件。

2） 示例：本地文件包含漏洞，可能需要管理员或具有某些权限的用户执行特定操作，或者软件配置错误。

e） 物理访问

1） 描述：攻击者必须能够直接或物理地接触目标系统，这可以是通过接入物理接口、硬件植入或直接盗用设备来实施。

2） 示例：需要直接访问计算机或服务器以使用 USB 引导恶意软件。

f） 特定版本或构建

1） 描述：漏洞只存在于特定版本的软件或固件中，或者仅在具有特殊构建环境时可被利用。

2） 示例：仅出现在某一特定操作系统内核版本中的驱动级漏洞，或者生产环境与开发环境不同，导致仅在生产环境上存在的安全问题。

g） 高级条件

1） 描述：利用涉及一系列复杂的前置条件，通常包括多个步骤、系统配置的连锁和多个变量。

2） 示例：攻击者需要引诱用户浏览一个含有恶意内容的网站，然后利用一个已知的浏览器漏洞来下载恶意软件，最终导致系统中毒，这整个过程中可能还会涉及绕过防火墙、安全软件或其他防护措施。

6.2 按照危害等级分级

a） 危害特别严重（危害程度系数：4）：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏。

b） 危害严重（危害程度系数：3）：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏。

c） 危害较大（危害程度系数：2）：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏。

d） 危害较小（危害程度系数：1）：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响。

6.3 按照修复难度分级

a） 修复难度非常高（修复难度系数：4）：恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的。

b） 修复难度高（修复难度系数：3）：恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的。

c） 修复难度较高（修复难度系数：2）：恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的。

d） 修复难度较低（修复难度系数：1）：恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。