T/EJCCCSE

团 体 标 准

T/EJCCCSE XXXX—XXXX

核电站网络安全防护技术要求与管理规范

Technical requirements and management norms for nuclear power plant network
security protection

(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

中国商业股份制企业经济联合会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 防护原则	2
6 基本要求	2
7 技术要求	3
8 管理要求	5

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。

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专利的责任。

本文件由中核核电运行管理有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：中核核电运行管理有限公司、××××、××××

本文件主要起草人：×××、××××××

核电站网络安全防护技术要求与管理规范

1 范围

本文件规定了核电站网络安全防护的原则、基本要求、技术要求和管理要求。

本文件适用于核电站系统生命周期的所有阶段网络安全活动,适用于指导核电站改善和提高网络安全防护能力。

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 22239	信息安全技术	网络安全等级保护基本要求
GB/T 22240	信息安全技术	网络安全等级保护定级指南
GB/T 25058	信息安全技术	网络安全等级保护实施指南
GB/T 25069	信息安全技术	术语
GB/T 28448	信息安全技术	网络安全等级保护测评要求
GB/T 28449	信息安全技术	网络安全等级保护测评过程指南
GB/T 32919	信息安全技术	工业控制系统安全控制应用指南
GB/T 37962	信息安全技术	工业控制系统产品信息安全通用评估准则
GB/T 37980	信息安全技术	工业控制系统安全检查指南

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全 *cybersecurity*

通过采取必要措施,防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。

3.2

访问控制 *access control*

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

3.3

管理信息大区 *management of information zone*

生产控制大区之外的,主要由企业管理、办公自动化系统及信息网络构成的安全区域。

3.4

生产控制大区 *production control zone*

由具有数据采集与控制功能,纵向联接使用专用网络或专用通道的电力监控系统构成的安全区域。

4 缩略语

下列缩略语适用于本文件。

B/S: 浏览器/服务器模式 (Browser/Server)
 C/S: 客户端/服务区模式 (Client/Server)
 FTP: 文件传输协议 (File Transfer Protocol)
 HTTP: 超文本传输协议 (Hyper Text Transfer Protocol)
 HTTPS: 以安全为目标的 HTTP 通道 (Hyper Text Transfer Protocol over Secure Socket Layer)
 Rlogin: 远程登录命令 (Remote Login in Unix Systems)
 SSH: 安全外壳协议 (Secure Shell)
 VLAN: 虚拟局域网 (Virtual Local Area Network)

5 防护原则

结合核电站系统特性和面临网络安全威胁，网络安全防护遵循以下基本原则：

- a) 核电站应参照本单位网络安全大纲等顶层文件和基本管理制度，指定和授权专门的部门对网络安全建设进行总体规划，制定近期和远期的安全建设工作计划；
- b) 应根据网络安全的等级划分情况，统一考虑网络安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件，应定期根据等保测评、风险评估的结果进行修订；
- c) 应组织相关部门和安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并向上级相关主管部门报备；
- d) 网络安全防护方案（总体安全策略、安全技术框架、总体建设规划、详细设计方案等相关配套文件）应确保在网络安全防护相应阶段工作开始前完成；
- e) 应根据核电厂工业控制系统的网络安全保护等级选择基本安全措施，并依据国家能源局、核安全局、公安部、国家卫生健康委员会等监管部门颁布的相关法令采取增强防护措施；
- f) 核电站应开展网络安全风险评估工作，并根据风险评估的结果对网络安全防护措施及时进行补充或调整；
- g) 核电站宜研究建立网络安全实验室或测试平台等基础设施，为上述安全防护方案、产品开发、洞补丁测试、变更验证等提供实验环境。

6 基本要求

6.1 网络安全机构

6.1.1 应明确由核电站主管网络安全工作的委员会或领导小组负责核电站系统网络安全领导工作，其负责人由企业法人或其授权代表担任。

6.1.2 应设立独立的行使系统网络安全管理职能的组织机构。

6.1.3 应制定文件明确网络安全机构的管理职责和各安全岗位的职责、分工和技能要求，以及确保机构内人员遵守机构的安全管理措施。

6.1.4 为保证各相关责任部门对各自的责任有一致的理解并明确所有重要职能，网络安全机构的组成和职责应经各系统责任部门联合审查确认。

6.2 网络安全人员

6.2.1 人员录用

6.2.1.1 应指定或授权专门的部门或人员负责网络安全相关岗位的人员录用工作。

- 6.2.1.2 应根据核电站的网络安全相关人员配备政策和现场网络安全防护工作需求制定人员录用计划及录用工作规程。
- 6.2.1.3 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。
- 6.2.1.4 应在人员任用前，在岗位描述、任用条款和条件中明确安全职责，并签署保密协议，协议内容包括网络安全的要求和责任。
- 6.2.1.5 应从内部人员中选拔从事网络安全相关的关键岗位人员。
- 6.2.1.6 应规定人员录用记录的保存时间，并按要求保存招聘过程和人员录用抉择的相关记录。

6.2.2 安全培训

- 6.2.2.1 应制定培训大纲、程序和课程，制定长期的培训和考核计划，并由核电站管理机构审核。
- 6.2.2.2 应定期对系统相关人员进行网络安全培训。
- 6.2.2.3 应定期对从事系统网络安全防护工作岗位的人员开展专业技能培训。专业技能培训内容应包含实际的安全防护技术练习，以模拟实际的系统网络安全攻击场景。
- 6.2.2.4 应定期（每年至少一次）对各类人员进行安全保密意识教育和岗位技能培训。
- 6.2.2.5 应定期开展网络安全意识培训，其内容应包括系统网络安全防护方针策略、安全操作程序、安全趋势和安全漏洞及其危害、识别和报告内部潜在威胁等。
- 6.2.2.6 应告知相关的网络安全责任和奖惩措施，确保所有从业人员意识到网络安全活动的相关性和重要性。

6.2.3 人员考核

- 6.2.3.1 应将核电站系统网络安全责任纳入人员考核体系。
- 6.2.3.2 应定期对系统各个岗位的人员进行安全技能及安全认知的考核。
- 6.2.3.3 应对关键岗位的人员进行全面、严格的安全审查和技能考核。
- 6.2.3.4 应按照企业保密制度定期对保密制度执行情况进行检查或考核。
- 6.2.3.5 应根据考核结果，对网络安全防护工作优异的人员进行奖励，对违反网络安全管理规定的的人员采取相应的惩罚措施。
- 6.2.3.6 应对考核结果进行记录并保存。

6.3 网络安全等级定级

核电站网络安全保护等级应与其重要性相匹配，具体的定级、备案、测评等要求应按 GB/T 22240、GB/T 28448、GB/T 28449、GB/T 25058 的规定执行。

7 技术要求

7.1 物理安全防护

- 7.1.1 核电站系统的机房应具有防震、防风、防雨、防潮、防火、防静电、防雷击、防电磁干扰、防辐照、核安保等措施。
- 7.1.2 机房应避免设在建筑物顶层或地下室以及用水设备的下层或隔壁
- 7.1.3 机房应配置电子门禁系统以加强物理访问控制，控制、鉴别和记录进入的人员，并对关键设备及磁介质实施电磁屏蔽。
- 7.1.4 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

7.2 分区分域及边界防护

- 7.2.1 生产控制大区与管理信息大区之间的通信应部署经国家主管部门检测认证的专用单向安全隔离装置。
- 7.2.2 严格禁止 E-mail、HTTP、Telnet、Rlogin、FTP 等安全风险高的网络服务和以 B/S 或 C/S 方式的数据库访问穿越专用横向单向隔离装置。
- 7.2.3 应具备对边界防护有效性进行实时监控和边界防护失效后及时报警的能力。
- 7.2.4 控制区与非控制区之间应采用具有访问控制功能的硬件工业防火墙，应具备逻辑隔离、报文过滤、访问控制等功能。
- 7.2.5 选用的工业防火墙应具备对流经控制区与非控制区工业控制通信协议进行过滤的功能，且不影响系统数据传输的响应要求。
- 7.2.6 生产控制大区内同属一个安全区域的各工业控制系统之间宜采用 VLAN 或访问控制等安全措施，限制系统间的直接互通。

7.3 通信网络安全

- 7.3.1 核电站应对生产控制大区的交换机、工业防火墙、单向隔离装置等网络设备、安全设备进行安全防护建设。
- 7.3.2 应对登录网络设备、安全设备的用户进行身份鉴别及权限控制，只允许相关管理、维护人员等登录设备。
- 7.3.3 对登录网络设备、安全设备应采用 HTTPS、SSH 等加密方式进行，同时辅以安全审计等管理措施。
- 7.3.4 网络设备、安全设备用户口令应该满足复杂度要求，定期更换，并由专人负责保护管理。
- 7.3.5 应及时清理网络设备、安全设备上临时用户、多余用户。
- 7.3.6 生产控制大区内应部署网络监控审计系统进行网络数据流监控审计，宜具备指令级监控审计能力。
- 7.3.7 生产控制大区和管理信息大区之间应部署网络入侵检测设备，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计。

7.4 计算环境安全

- 7.4.1 生产控制大区内主机应采用免受恶意代码攻击的技术措施。
- 7.4.2 生产控制大区内主机宜部署白名单软件和恶意代码防护软件，在部署或更新前，应首先在测试环境中测试通过，确保对业务系统无影响。
- 7.4.3 对不适宜部署恶意代码防护的主机，可通过部署主机白名单软件进行安全防护；应先在测试环境中进行充分测试，确保对业务系统无影响后方可实施；对列入白名单内的软件进程应遵循最小化原则。
- 7.4.4 可推广应用以密码硬件为核心的可信计算技术，用于实现计算环境和网络环境安全可信，免疫未知恶意代码破坏，应对高级别的恶意攻击。
- 7.4.5 生产控制大区内应部署安全审计设备，对操作系统、数据库、业务应用的重要操作进行记录、分析。
- 7.4.6 审计记录应包括事件的日期和时间、用户、事件类型，事件是否成功及其他与审计相关的信息。
- 7.4.7 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
- 7.4.8 应合理设置安全审计设备存储容量，保障安全审计日志保存时间不低于 6 个月。
- 7.4.9 采取上述安全增强措施前，应首先在测试环境中进行充分测试，确保所采取的措施对业务系统无影响。
- 7.4.10 应加强对安全增强措施的审核与管理，制定安全增强措施的技术要求和管理策略，充分发挥主

机增强措施的安全效应。

7.4.11 宜采用自主可控的安全增强系统实现以上要求。

7.5 可信验证

安全计算环境、安全区域边界、安全通信网络以及安全管理中心宜具备可信验证的能力。计算节点可基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，并将验证结果形成审计记录。

7.6 集中管控

7.6.1 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。

7.6.2 网络中的安全设备或安全组件应使用一条安全的信息传输路径进行管理。

7.6.3 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

7.6.4 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。

7.6.5 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

7.6.6 应能对网络中发生的各类安全事件进行识别、报警和分析。

7.6.7 应在专用场所建立集中的监控中心。

7.6.8 应独立实行系统管理、审计管理和安全管理。

7.7 核安全功能与网络安全功能原则要求

核电站系统的网络安全措施的实现不应影响核安全功能的实现，应考虑对系统的网络失效模式和失效后果影响，对系统的性能（包括响应时间）、有效性、可靠性或安全重要功能操作的影响应在设计安全规范范围内。

7.8 网络安全应急与核安全应急协调机制

7.8.1 应将核电站网络安全应急响应纳入应急管理体系中进行统一管理。

7.8.2 核电站应急组织的协调演练和紧急处理程序的演练不应影响核安全功能。

8 管理要求

8.1 管理体系

8.1.1 应按照“同步规划、同步建设、同步使用”（三同步）的原则，制定核电站网络安全总体方针和安全策略，建立网络安全管理制度，并将网络安全管理纳入日常安全生产管理体系。

8.1.2 工业控制系统与信息系统的共用安全管理，应沿用信息系统安全管理制度。信息系统安全管理制度不适用或未涉及工业控制系统的，应单独建立相应的工业控制系统安全管理制度。

8.1.3 应将网络安全纳入核电企业的核能安全、工业安全管理体系，加强能力建设，保障核电站网络安全。

8.1.4 应加强各类管理人员、内部组织机构和网络安全管理部門之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

8.1.5 宜加强与网络安全职能部门、各类供应商、业界专家和安全组织之间的沟通，并建立联系列表。

8.2 全生命周期安全管理

8.2.1 核电站系统及设备在规划设计、研究开发、施工建设、安装调试、运行管理、升级改造、退役报废等全生命周期的各阶段应采取相应安全管理措施。

8.2.2 宜采用安全可信的软硬件产品，供应商应保证所提供的设备及系统符合本文件、GB/T 22239、

GB/T 37962 的相关要求，并在设备及系统生命期内对此负责；专用安全防护产品的开发与使用，应按国家有关保密要求。

8.2.3 核电站系统及设备的运维单位应依据相关标准和规定进行安全防护专项验收；加强日常运维和安全管理，定期开展运行分析和自评估，符合 GB/T 37980、GB/T 32919 的相关要求，保障系统及设备的安全可靠运行；系统和设备退役报废时应按相关要求，销毁含敏感信息的介质和重要安全设备。

8.3 应急管理

8.3.1 核电站运营单位应将网络安全应急纳入应急管理体系中，内容应包括：目的、范围、角色、责任、管理层承诺、方针策略、制度、相关部门的协调、合规性等，并制定相应的应急响应预案：

- a) 应建立网络安全应急响应的组织，组织的负责人应为核电站生产运维领域或工业控制网络安全领域第一负责人；
- b) 运维工程师、核安全工程师和其他运行及支持人员应参与应急组织；
- c) 应明确安全事件类型及分类原则，确定各类安全事件的报告流程、响应和处理的范围、程度和处置方案等内容；
- d) 应急预案应包含全部可能发生的网络事件及导致的故障或问题；
- e) 应至少包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容，并明确系统应急需求、规定系统恢复优先级与目标、明确责任人等内容；
- f) 应对应急预案进行集中管理，避免发生泄露和未授权更改；
- g) 应制定应急培训和演练的计划，确保所有人员均进行了各自应急活动方面的培训和练习；
- h) 应急响应过程中形成的所有文档和记录均应妥善保存。

8.3.2 应急响应的方针策略、制度、计划，预案等规程性文档制定完成后，均应经过应急响应小组领导审核批准，如应急预案对应的安全事件可能引发核安全事件，该预案应经主管部门审查后，送交指定部门备案。

8.3.3 应明确规定应急响应的方针策略、制度、计划、预案等规程性文档需要定期进行审核和更新内容。

8.3.4 应针对系统或组织机构的变更或应急响应文档在实施、测试过程中遇到问题的情况，对应急响应文档进行审核和更新。

8.3.5 应定期对过去的网络安全事件进行总结提炼，将相应的改进行动落实到网络安全管理体系中。

8.3.6 应对全部人员进行应急响应培训，宣贯相应的政策、规程以及识别、响应疑似和确认的网络攻击事件和其他安全事件的方法。

8.3.7 应定期（每年至少一次）对应急响应工作人员进行专项应急培训，确保人员熟悉各自的应急响应任务。

8.3.8 应针对系统、组织机构或应急响应文档发生变更时，对应急响应工作人员进行专项培训，确保有关人员熟悉各自应急响应任务的变化。

8.3.9 应急培训时，应搭建模拟事件场景供受训人员进行实操练习。

8.3.10 应急响应文档审批通过后，应根据应急响应人员的职责，分发相应的应急响应文档。

8.4 安全事件管理

8.4.1 应对可能遭受的网络安全事件进行等级划分，并建立网络安全事件应急预案和现场处置方案。

8.4.2 应监控网络安全边界，以确保及时发现存在潜在的安全威胁并采取相应的措施。

8.4.3 应跟踪和记录系统内网络安全事件，对重要系统的异常事件重点监视。

8.4.4 应统计系统内网络安全事件的类型、频率和损害风险，并进行风险评估。

- 8.4.5 针对发现的网络安全事件相关的弱点、不足和脆弱性及可疑事件，任何发现事件的人员均应记录，并向应急响应机构或网络安全管理机构进行报告，但在任何情况下均不应尝试验证弱点。
 - 8.4.6 应定期组织网络安全机构与运行部门间关于系统网络安全事件的沟通交流。
 - 8.4.7 当网络安全事件可能导致涉及国家秘密的重大失、泄密事件时，应按照规定向相应的主管部门汇报。
 - 8.4.8 应具有应对网络安全事件的处理能力，涉及准备、检测、分析、控制、消除和恢复等方面工作，并应持续完善提升处置能力。
 - 8.4.9 应针对不同等级的网络安全事件采用不同的处理和报告程序。
 - 8.4.10 涉及国家秘密的网络安全事件应按照国家保密相关法规进行处置。
 - 8.4.11 在网络安全事件的报告和处置过程中，应分析和鉴定事件产生的原因，收集证据，记录处理过程。
 - 8.4.12 应通过对网络安全事件的评价分析，获取网络安全事件的特征经验，用于识别易重发的或高风险的事件，并采取必要措施避免类似事件重发。
 - 8.4.13 核电站系统应具备在规定的时间内，进行实时或准实时的恢复能力。
 - 8.4.14 应确保系统恢复后，系统运行状态与事件发生前一致。
 - 8.4.15 应跟踪核查系统状态，应确保处于规定的安全状态，否则应执行系统恢复工作。
-