核动力厂网络安全技术政策

（试 行）

一、 前言

核电厂营运单位（以下简称营运单位）必须对数字化技术的计算机、通信系统以及网络提供有效的保障，使其在遭受网络攻击时能够得到充分保护，以免对核安全、实物保护和应急响应产生不利影响。与这些功能相关的数字化技术的计算机、通信系统以及网络也必须受到保护，以应对网络攻击可能导致的数据或软件的可用性、完整性受到影响，或对系统、网络和相关设备的运行产生不利影响。

为实现上述目标，营运单位应建立、执行和维护网络安全大纲，同时应考虑影响该大纲实施的厂址特定条件。应使用和维持完整的纵深防御策略，以确保预防、检测和应对网络攻击，以及在受到网络攻击后减轻后果和恢复系统的能力，确保重要数字资产免受网络攻击的侵害。

制订本技术政策的目的在于指导营运单位通过建立和实施网络安全大纲，对核电厂网络安全风险进行监测和管理，以保证核电厂安全水平得以维持或得到提升。其他核设施营运单位可参照执行。

二、 网络安全大纲制定

为保护与核安全、实物保护和应急响应功能相关或提供支持的采用数字化技术的计算机、通信系统以及网络，应建立、实施

和维护网络安全大纲。

（一）建立网络安全大纲

1.定义岗位和职责并组建网络安全队伍

营运单位应组建网络安全队伍,并通过文件明确岗位、责任、权限和职能关系。网络安全队伍应由多学科、多领域工作经验的人员组成。典型的人员及其职责至少包括以下几类：

（1）网络安全责任人，其本身应为核电厂领导层管理人员，经授权对网络安全负有全面责任，负责大纲建立、批准，并为大纲的实施及维护提供必要资源。

（2）网络安全经理，履行以下主要职责：网络安全相关问题联络；监督并落实网络安全行动；组建并协调网络安全事故响应队伍；监督、制定和实施网络安全大纲、政策和程序；组织网络安全教育和培训。

（3）网络安全专家，履行以下主要职责：保护重要数字资产免受网络安全威胁；配置、运行和维护网络安全设备；对数字系统进行网络安全评估；对重要数字资产进行安全审核、漏洞评估、网络扫描和渗透测试；在重要数字资产遭受破坏后进行网络安全调查；保护在网络安全调查期间收集的证据及防止证据损坏和丢失；保持网络安全领域的专家技能和知识；为网络安全事件的预防和处置提供技术咨询和决策建议，必要时可聘请外部专家或机构。

（4）网络安全事件响应组织，包括实物保护、运营、工程、应急准备和其他外部支持人员，履行以下主要职责：在网络安全事件期间开展响应和行动，保护重要数字资产不受破坏，并协助恢复受

损系统；减轻涉及重要数字资产的网络安全事件造成的损失和危害，并确保事件发生后妥善恢复受影响的系统。

（5）辅助支持人员，包括负责操作、维护和设计数字系统的运行人员、工程师、技术人员、用户、承包商和供应商等。

2.识别重要数字资产

必须对数字化技术的计算机、通信系统和网络开展分析，以识别影响核安全、实物保护和应急响应功能的重要数字资产。

为识别重要数字资产，营运单位应首先确定与核安全、实物保护和应急响应功能或其支持功能相关的关键系统。

完成所有关键系统识别后，营运单位应分析和确定重要数字资产。重要数字资产可以是关键系统组件，可以是保护关键系统免受网络攻击组件，或者是可以直接或间接地连接到关键系统组件。

3.审查和确认

审查目的是审查和确认每个重要数字资产的直接和间接连接，识别重要数字资产路径，以确保重要数字资产部署在正确的安全区域、潜在的网络安全风险得到充分考虑、每个重要数字资产建立了初始配置。

进行审查的可行方法包括：

（1）识别和记录每个重要数字资产的物理和逻辑位置；

（2）识别和记录直接或间接连接重要数字资产的路径；

（3） 识别和记录重要数字资产基础设施间的相互依赖关系；

（4）确定和评估任何现有安全控制措施的有效性以及重要数字资产在网络安全架构中的位置。

通过对系统的物理和电气检查来确认信息,确认过程包括以下活动：

（1）对每个重要数字资产的配置进行物理检查，包括跟踪与重要数字资产连接的所有通信路径；

（2）检查为保护每个重要数字资产及其通信路径而建立的物理安全措施；

（3）沿着通信路径检查和评估网络安全控制（例如防火墙、入侵检测系统、网闸）的配置和有效性；

（4）检查与其他重要数字资产和关键系统的相关性，以及重要数字资产和关键系统之间的信任关系；

（5）检查与基础设施支持系统的相互依赖关系，尤其是供电、环境控制和消防设备的潜在危害；

（6）解决在审查过程中发现的信息或配置差异，包括未记录或连接被遗漏的情况，以及与重要数字资产和关键系统相关的其他违规行为。

（二）纵深防御策略

应使用和维持完整的纵深防御策略设计网络安全大纲，以确保预防、检测和应对网络攻击，以及在受到网络攻击后减轻后果和恢复系统的能力。

必须采用纵深防御策略来确保重要数字资产免受网络攻击的侵害。可结合网络安全架构建立连接边界，并部署防御措施来保护、探测、响应、缓解对重要数字资产攻击，并在受到攻击后恢复。

（三）安全控制

应对网络安全控制执行有效性和脆弱性分析，以确保重要数字资产在遭受网络攻击时得到防护。如存在缺陷，应采取额外的网络安全控制措施。

不应使用会对核安全、实物保护和应急响应功能或性能产生不利影响的安全控制措施（例如，系统响应时间的不可接受的变化，系统复杂性的不良增长）。当安全控制措施会产生不利影响时，营运单位应采用替代措施，以确保重要数字资产得到防护。任何因上述情况导致的脆弱性都应通过替代控制措施消除或缓解。

1.技术控制

技术控制是硬件、固件、操作系统或应用软件中包含的非人员执行的预防或防护措施。技术控制包括访问控制、审计和追溯、系统和通信保护、身份识别和身份认证、系统加固等。技术控制动作是预先设计和预编程的，并根据触发事件自动执行，通常不需要人为干预。

2.操作控制

操作控制是人员执行的保护措施，而非设备自动执行的。操作控制包括涉及存储介质保护、物理和环境保护、人员安全、系统和信息完整性、应急计划、事件响应、维护、缓解攻击、功能连续性、培训以及配置管理的活动。操作控制应有文档化的规程，以确保核电厂人员和承包商对其行为负责。

3.管理控制

管理控制是专注于风险管理和网络安全大纲的控制。系统或服务采购、网络安全评估和风险管理、数字资产的增加和修改等活动

均属于管理控制范畴。

三、 网络安全大纲实施和维护

应定期进行网络安全风险评估和管理，为重要数字资产制定全生命周期的网络安全措施，包括持续监测和评估、配置管理、变更管理、变更与环境的安全影响分析、有效性分析、持续评估网络安全控制和安全大纲的有效性、脆弱性扫描、脆弱性评估、变更控制、安全大纲审查等。

（一）持续监测和评估

应开展持续监测和评估，并考虑网络安全技术进步，确保针对安全控制、相关流程和程序建立定期审查和试验的安全控制措施持续有效，系统、网络、环境的变化或新出现的威胁不会降低原有措施的效果。持续监测包括：持续评估以确认每个重要数字资产实施的安全控制措施在整个生命周期内保持有效；确保未经授权的资产未连接到基础设施；对安全控制的必要性和有效性的持续评估；定期的网络安全大纲审查、评估和提高安全计划的有效性。

根据持续监测和评估结果更新网络安全大纲，以反映必要的更改，保证重要数字资产得到充分保护。

（二）变更控制

变更控制是管理网络安全的关键要素，应开展变更控制确保增加或修改的重要数字资产以受控和协调的方式引入。有效的变更控制所需的文件至少包括：标识了授权和实施更改人员的配置项变更日志、变更日期和时间、变更目的、安全控制有效性的验证以及在变更过程中的监测记录等。

1.配置管理

应对整个生命周期内重要数字资产的变更进行控制以确保网络安全大纲目标得到满足。在重要数字资产生命周期的运行和维护阶段，使用有效的配置管理确保对重要数字资产的更改按照流程和程序进行，不会在系统中引入额外的安全风险。配置管理还应保证营运单位及时有效地执行变更控制。营运单位应在实施变更之前对重要数字资产的变更进行评估，以确保维持网络安全目标。

2.安全影响分析

安全影响分析有助于管理由系统、网络、环境或新出现的威胁所引起的潜在漏洞、薄弱环节和风险。应在重要数字资产设计、配置变更或其环境发生变化之前执行安全影响分析，并进行评估和记录。同时将其他受影响的重要数字资产或系统纳入网络安全影响分析，并更新和记录以下内容：重要数字资产和其关联资产的位置；连通路径（直接和间接）；基础设施相互依赖关系；防御性策略，包括网络安全架构、安全控制和其他防御性策略措施；物理和网络安全策略及程序文件，包括攻击缓解、事件响应和系统恢复；用于筛选、评估、减轻和处理从可信来源收到的威胁和漏洞通知的程序。

应将这些影响分析作为变更批准过程的一部分来执行，以评估变更对重要数字资产的网络安全态势的影响，应在完成分析后实施新的安全控制措施。

（三）网络安全大纲审查

营运单位应为网络安全大纲配套制定必要的措施和管理程序，并执行对大纲要素的审查。审查方法包括：制定和实施审查计划；

制定和执行维护网络安全大纲的实施程序。

必须记录网络安全大纲审查的结果和意见、管理层关于大纲有效性的整改意见以及任何因先前程序审查的意见而采取的行动。以可审核的形式进行网络安全大纲维护，根据要求供检查使用。

四、 保存记录

应保存的记录包括但不限于所有收集、记录与分析网络和重要数字资产事件或事故的数字记录、日志文件、设计文件和非数字文件。保留上述记录和支持性技术文件，是为确保检查人员、审计人员或者技术支持人员能够对网络安全大纲所描述的、引用的或包含的事件，以及其他与网络安全大纲各个要素相关的活动进行评估。

必须保留所有记录和技术支持文件，在记录被取代后至少还应保存 3 年。

五、 监管要求

营运单位应至少每 24 个月完成一次网络安全大纲审查。在以下情况出现时应开展审查：在大纲初次实施 12 个月内；运行环境变化可能对安全产生不利影响；基于厂址特定分析、评估或其他绩效指标按需开展。

网络安全大纲应纳入保密管理，必要时国务院核安全监督管理部门、国务院核工业主管部门可对网络安全大纲进行检查和评估。

建立网络安全大纲并维持核电厂网络安全是一项必要且长期的工作，需要不断优化完善。国务院核安全监督管理部门、国务院核工业主管部门将根据职责分工，逐步推进核电厂网络安全相关工作，并持续完善相关核安全要求。

附录

名　词　解　释

1.网络攻击

计算机和通信系统与网络的物理或逻辑威胁的一种表现形式。包括试图对重要数字资产和/或关键系统的服务、资源或信息进行未经授权的访问，试图破坏对重要数字资产和/或关键系统的完整性、可用性或保密性，或试图对核安全、实物保护和应急响应造成不利影响。

2.关键系统

核电厂中与核安全、实物保护和应急响应相关的基于模拟或数字技术的系统，包括但不限于核电厂系统、设备、通信系统、网络、场外通信或支持系统或设备。

营运单位应对这些关键系统、设备、通信和网络进行初步影响分析，以确定其中哪些在失效情况下会影响核安全、实物保护和应急响应功能。分析不应考虑现有的缓解措施，以确定可能的最不利影响。

关键系统包括：

（1） 执行或支持核安全、实物保护和应急响应功能的系统；

（2）影响核安全、实物保护和应急响应功能或影响关键系统和/或重要数字资产执行相关功能的系统；

（3）为上述系统和/或重要数字资产遭受网络攻击提供路径的

系统，通过该系统提供的路径可能导致核安全、实物保护和应急响应功能损害、降级；

（4）上述系统和/或重要数字资产的支持系统；

（5）保护上述任何系统免受网络攻击的系统。

对于与核安全、实物保护和应急响应功能不直接相关的支持系统或设备，营运单位应开展相关性分析，如分析表明会造成不利影响，也应是关键系统。

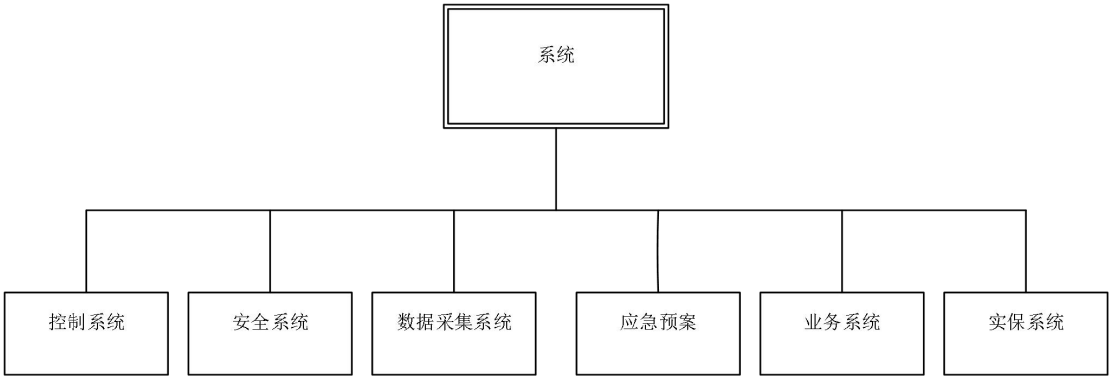

图 1　核安全、实物保护和应急响应功能相关的通用分类

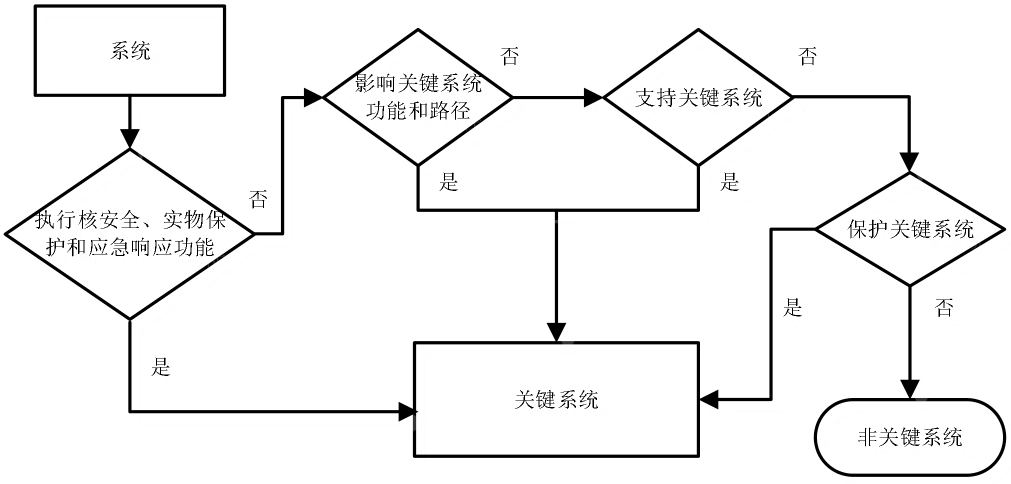

图 2　关键系统的评估过程

图 1 展示了核电厂中关于核安全、实物保护和应急响应功能相关系统的通用分类，这些系统的失效可能导致放射性释放（例如严重的堆芯损坏），并对公众健康和安全产生不利影响。

3.重要数字资产

由数字化计算机、通信系统以及网络组成或包含数字化计算机、通信系统及网络的关键系统的子组件。

识别重要数字资产前应对核电厂内的所有系统进行广泛评估。

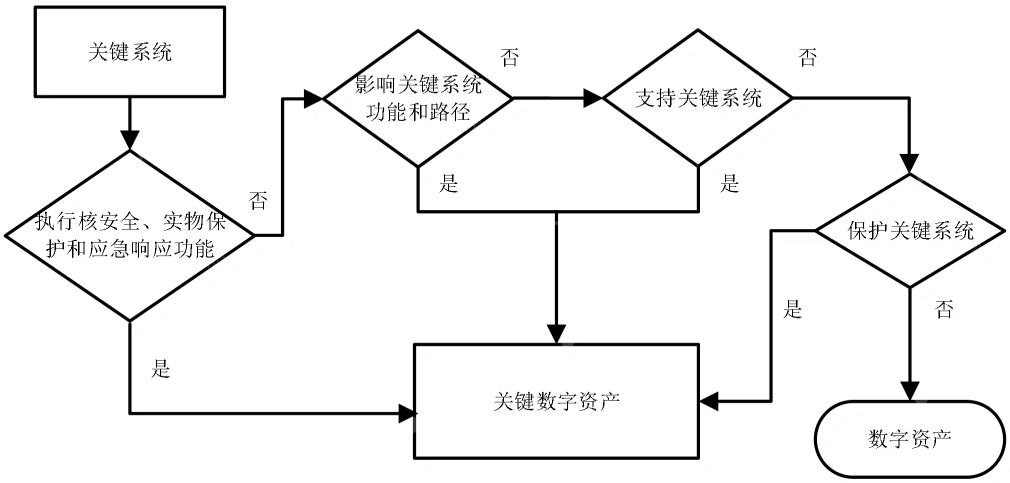

图 3　重要数字资产的评估过程

重要数字资产包括：

（1）执行核安全、实物保护和应急响应功能的数字资产；

（2）可能对核安全、实物保护和应急响应功能，或执行相关功能的关键系统和/或重要数字资产产生不利影响的数字资产；

（3）为关键系统和/或重要数字资产遭受网络攻击提供路径的数字资产，通过该数字资产提供的路径可能导致核安全、实物保护和应急响应功能损害、降级；

（4）支持关键系统和/或重要数字资产的数字资产；

（5）保护上述任何数字资产免受网络攻击的数字资产。

为识别重要数字资产，营运单位应收集以下信息：

（1）每个系统、资产或网络的简要描述；

（2）每个重要数字资产和关键系统总体功能的简要描述；

（3）重要数字资产或关键系统遭到破坏的潜在后果；

（4）重要数字资产的功能；

（5）每个关键系统内的重要数字资产；

（6）网络安全功能要求和规范说明，包括：开发和评估相关的质保要求、系统开发商或供应商必要的网络安全要求。

4.重要数字资产基础设施

关于核电厂重要数字资产基础设施，通常认为数字化控制系统（包括安全级与非安全级的）以及棒控、多样化反应堆保护系统、实物保护、应急等整体系统都应纳入重要数字资产基础设施。对于在国内核电厂普遍应用的安全级数字化控制系统和相关功能模块中的专用芯片、传感器、可编程序逻辑控制器、组态软件等都可以认为是重要数字资产的基础设施。

附件

主 送 单 位 名 单

序 号	单　　位
1	生态环境部华北核与辐射安全监督站
2	生态环境部华东核与辐射安全监督站
3	生态环境部华南核与辐射安全监督站
4	生态环境部东北核与辐射安全监督站
5	生态环境部核与辐射安全中心
6	国家核安保技术中心
7	机械科学研究总院核设备安全与可靠性中心
8	苏州热工研究院
9	北京核安全审评中心
10	上海核安全审评中心
11	中国核工业集团有限公司
12	中国核能电力股份有限公司
13	中国广核集团有限公司
14	国家电力投资集团有限公司
15	中国华能集团有限公司
16	中国核电工程有限公司
17	中广核工程有限公司
18	上海核工程研究设计院
19	华龙国际核电技术公司
20	中核武汉核电运行技术股份有限公司
21	中核核电运行管理有限公司

序 号	单　　位
22	江苏核电有限公司
23	福建福清核电有限公司
24	三门核电有限公司
25	海南核电有限公司
26	大亚湾核电运营管理有限责任公司
27	辽宁红沿河核电有限公司
28	福建宁德核电有限公司
29	阳江核电有限公司
30	台山核电合营有限公司
31	广西防城港核电有限公司
32	中广核惠州核电有限公司
33	山东核电有限公司
34	国核示范电站有限责任公司
35	华能山东石岛湾核电有限公司
36	中核国电漳州能源有限公司