ICS 27.120.20
CCS N 18

中华人民共和国国家标准

GB/T 41241—2022

核电厂工业控制系统网络安全管理要求

Management requirements for cybersecurity of industrial control systems in nuclear power plant

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

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。

本文件由全国核仪器仪表标准化技术委员会(SAC/TC 30)提出并归口。

本文件起草单位：中广核工程有限公司、中国广核电力股份有限公司、上海核工程研究设计院有限公司、江苏核电有限公司、核工业标准化研究所、清华大学、中核武汉核电运行技术股份有限公司、福建福清核电有限公司、北京广利核系统工程有限公司、大亚湾核电运营管理有限责任公司、辽宁红沿河核电有限公司、奇安信科技集团股份有限公司、山石网科通信技术股份有限公司、深信服科技股份有限公司、中国核电发展中心。

本文件主要起草人：谭珂、吴挺、黄伟军、颜振宇、李贤民、谢红云、刘高俊、春增军、杨晓晨、李若兰、郭智武、周亮、彭华清、张淑慧、毛磊、郑威、徐霞军、王略、赵磊、刘学科、梁雪元、金武剑、李志忠、张人友、高汉军、曲鸣、蔡红伟、卢俊、刘元、石秦、李实、李广峰、关峻峰、张天元、晏培、刘太洪、罗东平、胡兵、陈薇。

引　言

为提升和规范核电厂工业控制系统的网络安全防护能力，根据国家在电力监控系统网络安全防护的要求和规定、电力行业信息系统安全等级保护基本要求、核电厂仪表和控制系统相关核安全导则等方面的要求，制定本文件。

核电厂工业控制系统网络安全管理要求

1 范围

本文件规定了核电厂工业控制系统网络安全方面的管理、技术防护和应急管理的要求。

本文件适用于核电厂领域工业控制系统生命周期的所有阶段(包括设计、开发、工程实施、运行和维护、退役等)网络安全活动,也适用于指导核电厂工业控制系统用户改善和提高生产系统中网络安全防护能力的系统维护活动。

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 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 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

3 术语和定义

下列术语和定义适用于本文件。

3.1

验收 acceptance

风险评估活动中用于结束项目实施的一种方法,主要由被评估方组织机构,对评估活动进行逐项检验,以是否达到评估目标为接受标准。

[来源:GB/T 30976.1—2014,3.1.4]

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。

[来源:GB/T 25069—2010,2.2.1.42]

3.3

鉴别 authentication

验证实体所声称的身份的动作。

[来源:GB/T33009.1—2016,3.1.2]

3.4

可用性 availability

数据或资源的特性,能被授权实体按要求访问和使用数据或资源。

[来源:GB/T 20984—2007,3.3]

3.5

保密性　confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[来源：GB/T 20984—2007，3.5]

3.6

控制区　control sub zone

由具有实时监控功能、纵向联接使用电力调度数据网的实时子网或者专用通道的各业务系统构成的安全区域。

[来源：GB/T 36572—2018，3.4]

3.7

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。

[来源：GB/T 22239—2019，3.1]

3.8

网络安全措施　cybersecurity measures

为保护资产、抵御威胁、减少脆弱性、降低网络安全事件的影响而实施的各种实践、规程和机制。

3.9

识别　identify

对某一评估要素进行标识与辨别的过程。

[来源：GB/T 30976.1—2014，3.1.2]

3.10

信息系统　information system

有计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

注：典型的信息系统由三部分组成：硬件系统（计算机硬件系统和网络硬件系统）；系统软件（计算机系统软件和网络系统软件）；应用软件（包括有其处理、存储的信息）。

[来源：GB/T 20984—2007，3.8，有修改]

3.11

完整性　integrity

保证信息及信息系统不会被非授权更改或破坏的特性。

注：包括数据完整性和系统完整性。

[来源：GB/T 20984—2007，3.10，有修改]

3.12

管理信息大区　management 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。

[来源：GB/T 36572—2018，3.6]

3.13

非控制区　non-control sub zone

在生产控制范围内由在线运行但不直接参与控制、是电力生产过程的必要环节、纵向联接使用电力调度数据网的非实时子网的各业务系统构成的安全区域。

[来源：GB/T 36572—2018，3.5]

3.14

组织　organization

由作用不同的个体为实施共同的业务目标而建立的机构。

注：一个单位是一个组织，某个业务部门也可以是一个组织。

[来源：GB/T 20984—2007，3.11，有修改]

3.15

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。

[来源：GB/T 36572—2018，3.3]

3.16

残余风险　residual risk

采取了安全措施后，信息系统仍然可能存在的风险。

[来源：GB/T 20984—2007，3.12]

3.17

风险分析　risk analysis

系统地使用信息来识别风险来源和估计风险。

[来源：GB/T 30976.1—2014，3.1.8]

3.18

风险评估　risk assessment

系统地辨识重要系统资源的潜在脆弱性和威胁，基于发生的概率量化损失风险和后果，并（可选地）建议如何对各对抗措施分配资源以使总风险最小的过程。

注 1：资源类型包括物理资源，逻辑资源和人力资源。

注 2：风险评估常与脆弱性评估相结合，以辨识脆弱性并量化相关风险。周期地执行这些内容是为了反映组织机构的风险裕度、脆弱性、规程、人员和技术上的变化。

[来源：GB/T33009.3—2016，3.1.18]

3.19

安全系统　safety systems

安全上重要的系统，用于保证反应堆安全停堆、从堆芯排出余热或者限制预计运行事件和设计基准事故后果。

[来源：GB/T 15474—2010，3.7]

3.20

网络安全事件　cybersecurity incident

可能会造成网络安全策略的违反、防护措施的失效，或进入未预知的不安全状况的系统、服务或网络的一种可识别状态。

3.21

威胁　threat

可能导致对系统或组织危害的不希望事故潜在起因。

[来源：GB/T20984—2007，3.17]

3.22

脆弱性　vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安保策略。

[来源：GB/T 30976.1—2014，3.1.1]

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/服务器模式(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)

5 核电厂工业控制系统网络安全管理

5.1 网络安全管理通用要求

5.1.1 管理体系的建立

本项要求包括：

a) 应根据网络安全法的要求，按照“同步规划、同步建设、同步使用”(三同步)的原则，制定核电厂工业控制系统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；

b) 工业控制系统与信息系统能共用的安全管理制度，应沿用信息系统安全管理制度；

c) 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；

d) 应将工业控制系统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，保障核电厂工业控制系统网络安全；

e) 宜加强各类管理人员、内部组织机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

f) 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。

5.1.2 安全管理及防护原则

本项要求包括：

a) 核电厂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工业控制系统的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) 应根据工业控制系统的等级划分情况，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) 核电厂应开展工业控制系统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) 核电企业宜研究建立核电厂工业控制系统的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、漏洞补丁测试、变更验证等提供实验环境。

5.1.3 制度体系维护

本项要求包括：

a) 应制定相关管理制度，明确核电厂工业控制系统网络安全管理制度的制定、发布、修订、维护等事项的管理要求；

b) 应明确工业控制系统网络安全管理制度执行责任的主体部门和人员；

c) 工业控制系统网络安全管理制度应通过正式、有效的方式发布，并进行宣贯，并注明发布范围；

d) 应定期组织相关部门和相关人员对工业控制系统网络安全管理制度的合理性和适用性进行评估，对存在不足或需要改进的管理制度进行修订。

5.1.4 安全管理机构

本项要求包括：

a) 应明确由核电企业主管网络安全工作的委员会或领导小组负责信息系统网络安全与工业控制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；

b) 应设立独立的行使工业控制系统网络安全管理职能的组织机构；

c) 应制定文件，明确安全管理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；

d) 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，网络安全管理机构的组成和职责应经各工业控制系统责任部门联合审查确认。

5.1.5 安全管理岗位

本项要求包括：

a) 核电厂应设立系统管理、安全管理、审计管理等网络安全岗位，明确各部门及工作岗位的职责；

b) 核电厂应配备一定数量的系统管理员、审计管理员和安全管理员等，并根据实际需求设置专职岗位；

c) 系统管理员、安全管理员、审计管理员不可互相兼任。

5.1.6 网络安全人员管理

5.1.6.1 人员录用

本项要求包括：

a) 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；

b) 应根据核电厂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；

c) 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；

d) 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；

e) 应从内部人员中选拔从事网络安全相关的关键岗位人员；
f) 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。

5.1.6.2 人员考核

本项要求包括：
a) 应将工业控制系统网络安全责任纳入人员考核体系；
b) 应定期对工业控制系统各个岗位的人员进行安全技能及安全认知的考核；
c) 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；
d) 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；
e) 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人员采取相应的惩罚措施；
f) 应对考核结果进行记录并保存。

5.1.6.3 人员离岗

本项要求包括：
a) 应针对工业控制系统人员离岗制定相应的管理制度；
b) 应及时终止工业控制系统离岗人员的所有访问权限，取回所有身份证件、钥匙、徽章等以及机构提供的软硬件设备；
c) 应终止离职人员对工业控制系统的使用权限；
d) 网络安全管理层和关键岗位人员调离岗位，应根据离岗单位相关的保密管理要求和流程执行，并进行离岗安全审查，办理移交手续。

5.1.6.4 外部人员管理

本项要求包括：
a) 应建立关于外部人员的管理制度，明确包含安全角色和责任的人员安全要求，并形成文件；
b) 应在外部人员进入现场开展工作前，进行入场培训，并签署保密协议；
c) 应确保在外部人员物理访问受控区域前提出书面申请，批准后由专人全程陪同，并登记备案；
d) 应确保在外部人员接入网络访问系统前提出书面申请，批准后由专人开设账号、分配权限，并登记备案；
e) 外部人员离场后应及时清除其所有访问权限。

5.1.7 安全培训

本项要求包括：
a) 应制定培训大纲、程序和课程，制定长期的培训和考核计划，并由核电企业管理机构审核；
b) 应定期对工业控制系统相关人员进行工业控制系统网络安全培训；
c) 应定期对从事工业控制系统网络安全防护工作岗位的人员开展专业技能培训；
d) 专业技能培训内容应包含实际的安全防护技术练习，以模拟实际的工业控制系统网络安全攻击场景；
e) 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；
f) 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；
g) 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；

h） 应妥善保存培训过程中的各项记录。

5.2 设计阶段管理要求

5.2.1 设计管理

本项要求包括：

a） 应按照“三同步”原则将工业控制系统网络安全贯穿于核电厂设计活动；

b） 应明确核电厂工业控制系统的网络安全保护等级及相关安全需求；

c） 应在核电厂工业控制系统初始设计阶段包含工业控制系统网络安全防护设计；

d） 在安全设计环节应针对工业控制系统的网络安全防护需求，综合考虑工业控制系统安全性、可靠性、可维护性；

e） 应包含工业控制系统网络安全防护的详细设计。

5.2.2 设计变更

本项要求包括：

a） 应编制相关制度，用于明确核电厂工业控制系统网络安全设计环节变更的工作流程；

b） 工业控制系统网络安全设计变更应经过充分的论证，并制定相应的变更验证方案及恢复措施；

c） 对于执行核安全或核安全有关功能的工业控制系统，其网络安全设计变更应有严格内部审核过程，并根据规定报相关核安全监管部门；

d） 应对设计变更后系统的网络安全风险进行评审，并确认风险控制在可接受范围内；

e） 应根据变更后对系统网络安全防护方面的影响，进行相应的网络安全防护变更设计。

5.2.3 设计验证

本项要求包括：

a） 应根据网络安全设计文档明确设计验证计划，明确验证节点、验证方式等关键内容，并编制验证文档；

b） 网络安全设计验证应采用评审、审核、分析、测试等方法或这些方法的组合；

c） 工业控制系统网络安全设计验证工作应从系统研制阶段即开展，贯彻整个设计环节，与设计工作并行开展。

5.2.4 网络安全等级保护定级

核电厂工业控制系统网络安全保护等级应与其重要性相匹配，具体的定级、备案、测评等要求按照GB/T 22240、GB/T 28448、GB/T 28449、GB/T 25058执行。

5.3 采购阶段管理要求

5.3.1 采购管理

本项要求包括：

a） 应编制相关制度，明确采购工作的相关管理要求，确保准确提出涉及网络安全的设备、产品及服务的采购技术要求；

b） 应指定相关部门负责产品和服务的采购工作，包含申报、审核、立项、采购、验收等环节。

5.3.2 产品规范

本项要求包括：

a) 应确保采购的网络安全产品或服务符合国家的相关要求，并通过国家网络安全相关部门评估，具有网络安全保障和网络安全管理的相关功能；
b) 应确保采购用于工业控制系统的网络安全产品，通过国家认可机构的安全性检测和电磁兼容性的检测；
c) 应用于核电厂工业控制系统内的网络安全防护产品，应在使用前进行充分验证，确保其不影响工业控制系统的可靠性和稳定性后方可应用于现场；
d) 计划应用于安全级工业控制系统的网络安全防护产品，应具备工业网络安全相关产品资质，符合自主可控安全可信要求；
e) 应确保采购的密码产品符合国家密码管理规定。

5.3.3 供应商管理

本项要求包括：
a) 应确保网络安全产品供应商的选择符合国家的有关规定；
b) 应明确供应商所需履行的网络安全义务和防护措施，通过评审、检查、测试等方式确保供应商网络安全防护措施的有效性；
c) 应与供应商签订保密协议；
d) 在满足功能、性能要求的前提下应优先采用自主可控的工业控制系统及其网络安全相关产品。

5.4 建设阶段管理要求

5.4.1 建设管理

本项要求包括：
a) 应制定相关制度，明确工业控制系统建设环节中实施过程的管理方式和人员行为准则等内容；
b) 建设环节的网络安全防护措施应满足设计文件要求，并明确建设阶段的网络安全管理要求；
c) 应为建设环节各重要节点设置明确验证节点，验证通过后方可开展后续建设工作，验证报告应留档保存，用于项目审核追溯。

5.4.2 验收管理

本项要求包括：
a) 应由工业控制系统建设方对系统进行网络安全性测试，并提供可供复查的安全测试报告，由业主单位进行审核和确认；
b) 应由核电厂委托具有相关资质的独立第三方测评机构对系统进行网络安全测试，并出具安全测试报告；
c) 应验证系统集成的网络安全防护功能不影响系统的正常运行，部署的独立安全工具应在部署前先进行兼容性测试，对可能造成影响的情况，应由建设方进行处理；
d) 进行渗透性测试的测试环节，应由业主单位和系统建设方进行沟通确认，并进行备份做好恢复准备措施；
e) 系统测试环境应独立于系统运行环境和开发环境；
f) 系统测试过程中应避免使用个人信息或其他敏感信息，并保障测试用运行数据的安全性。

5.4.3 交付管理

本项要求包括：
a) 应制定相关制度，明确交付环节的管理要求和人员行为准则等内容；

b) 应制定详细的交付清单，明确需交接的硬件、软件和文档等资产；
c) 应指定专人负责系统交付后的网络安全管理；
d) 应交付系统网络安全相关的文档资料；
e) 应对负责系统运行管理的部门和人员进行相应的培训。

5.5 运行阶段管理要求

5.5.1 环境管理

本项要求包括：

a) 应建立关于工业控制系统运行环境安全管理制度，对有关工业控制系统运行环境物理访问，物品出入控制等方面的管理要求做出规定，并定期对工业控制系统运行环境供配电、空调、温湿度控制等设施进行维护管理；
b) 应对工业控制系统运行环境的出入人员进行相应级别的授权，对进入重要安全区域的活动行为进行实时监视和记录；
c) 应指定专门的部门或人员定期对工业控制系统运行环境物理访问记录进行检查；
d) 应指定专门的部门或人员在发生事件或发现事件迹象的情况下对工业控制系统运行环境物理访问记录进行检查。

5.5.2 资产管理

本项要求包括：

a) 应建立资产安全管理制度，规定系统资产管理的责任人员或责任部门，对资产分类、标识方法做出规定，并对资产的使用、传输和存储等进行规范化管理；
b) 编制并维护所有重要资产的清单，资产清单要包括资产责任部门、责任人、重要程度和所处位置等所有为从灾难中恢复而必要的信息；
c) 应确保采用的资产标识方法满足标识清楚且不能涂改的要求，且不影响资产正常使用的要求，资产标记应包括物理和资料格式的资产；
d) 应根据资产的重要程度对资产进行颜色醒目标识度区分管理，涉及网络安全系统及其部件应唯一标识，并根据资产的价值选择相应的管理措施。

5.5.3 变更管理

本项要求包括：

a) 应建立工业控制系统网络安全相关变更的管理制度，并建立关于变更申请和审批的程序，并留存记录；
b) 应充分论证变更的必要性和可行性，针对安全级工业控制系统，在变更前应根据相关规定通过监管部门的审批；
c) 应根据变更需求制定变更实施方案，针对安全级工业控制系统的变更，实施前应开展模拟验证；
d) 应充分论证变更实施过程对系统安全的影响，并制定必要的应对措施和预案，以确保变更不引入新的安全风险；
e) 变更的执行人员应进行严格的授权考核，仅有资质的人员能够执行变更操作。

5.5.4 存储介质及连接管理

本项要求包括：

a) 应建立存储介质安全管理制度，对存放环境、使用、维护和销毁等方面做出规定；
b) 存储介质应集中存放并指定专人管理，建立资产台账，定期盘点；
c) 存储介质的使用应采用“借用审批，归还确认”的制度，并严格控制其在工业控制系统中的使用；
d) 应用于不同系统中的存储介质应有清楚地标识，并将其使用严格限制在所应用的系统中；
e) 存储介质在使用前应在专用杀毒计算机上杀毒，并留存杀毒记录；
f) 应关闭、拆除或封堵控制系统设备上不需使用的软盘驱动、光盘驱动、USB 接口、串行接口或多余网口等，确需保留的应通过相关的技术控制措施实施严格的监控管理；
g) 应确保存储介质存放在安全的环境中，保存环境应符合所存储数据等级的物理安全防护要求；
h) 应根据管理制度要求对存储介质的使用、维护和销毁等工作进行严格管理，并对管理过程进行记录；
i) 应对送出维修的存储介质进行跟踪记录，在送修前应清除敏感或秘密数据；
j) 应对销毁的存储介质清除敏感或秘密数据，采用物理销毁和消磁处理，并指定专人跟踪；
k) 应用于不同系统中移动设备应有清楚地标识，应包含责任人，系统信息等，并严格限制在所应用的系统中；
l) 应禁止未经授权的移动设备开启无线功能。

5.5.5 网络和系统管理

本项要求包括：

a) 应建立网络和系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程、补丁与升级、口令更新周期等方面做出规定；
b) 应依据操作手册对系统进行安全维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
c) 根据业务重要性的不同，应设置有不同权限的用户进行网络和系统的运维管理，并经过严格的授权考核；
d) 系统应配备相应的管理人员，在必要时能阻断各层网络边界上异常的通信线路；
e) 应严格控制运维工具的使用，经审批后方可接入进行操作，操作过程中应保留审计日志；
f) 应对通信线路、主机、网络设备和应用软件的运行状况、网络行为等进行监测和报警，形成记录并妥善保存；
g) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
h) 应对系统资源的使用进行监控，以确保充足的处理速度和存储容量，管理人员应随时掌握系统资源的使用情况，包括处理器、存储设备和输出设备。

5.5.6 无线使用管理

应严格评估无线通信技术应用于核电厂工业控制系统的安全性，在确保安全的前提下谨慎使用。

5.5.7 远程接入管理

不应在核电厂工业控制系统中使用远程接入管理功能。

5.5.8 账户管理

本项要求包括：

a) 应建立账户管理流程与策略，应对系统账户管理流程与策略进行评审；
b) 应指定专门的部门或人员进行账户管理；

c) 应及时对所有账户进行检查，核查账户的分配是否经过管理员授权、审批。

5.5.9 口令管理

本项要求包括：

a) 应制定口令管理制度，对各类用户的口令进行管理；
b) 口令应根据工业控制系统及设备特点规定有效期和口令强度要求；
c) 应将存储用户口令的存储介质保存在实施严格物理访问控制的安全位置；
d) 应使用安全的方式为用户分配用户及口令，应避免信息泄露，并要求用户确认接收；
e) 应在分配用户时仅设置安全的临时口令，并强制用户立即更改；
f) 应对登录的用户进行身份标识和鉴别，按照系统定级采取相应的系统登、离措施，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
g) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和登录连接超时自动退出等相关措施。

5.5.10 权限管理

本项要求包括：

a) 应针对用户的访问权限制定相应的管理制度，包括用户权限的分配、变更、注销和审核；
b) 用户初始化创建时应不具备任何权限，仅由管理人员根据用户的业务功能需求分配最小权限；
c) 应明确标识系统内全部的特殊权限（包含操作系统、数据库系统和业务应用程序等），以及需要具备这些特殊权限的用户；
d) 特殊权限要按照访问控制策略在“按需使用”和“一事一议”的基础上分配给用户，即仅当需要时，为其职能角色分配最低要求权限，使用结束后立刻撤销权限；
e) 应根据用户的岗位变动，重新分配相应用户的访问权限并进行审核。

5.5.11 补丁及漏洞管理

本项要求包括：

a) 应建立并实施关于系统、设备的补丁和漏洞管理程序，并制定工业控制系统补丁安装流程；
b) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后决定是否进行修补；
c) 应评估并确定补丁安装对系统安全的影响，确保补丁安装后系统能够满足目标安全等级；
d) 安装系统补丁程序或升级设备程序前，应在测试环境中测试通过后，并对重要文件进行备份，方可实施系统补丁程序的安装，补丁安装前应做好应急方案；
e) 补丁升级工作应安排在系统空闲时间，减少对系统业务功能稳定运行的影响。

5.5.12 备份与恢复管理

本项要求包括：

a) 应建立备份与恢复管理相关的安全管理制度，明确备份策略，对备份方式、备份频率、存储介质和保存期等进行规范；
b) 应根据数据所属系统的重要性及其对核电厂工业控制系统的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序，备份策略指明备份数据的放置场所、文件命名规则、存储介质替换频率等；
c) 应根据系统的数据备份策略，制定相应的灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，对不适用的规定进行修改或更新；

d) 应识别系统信息的重要级别，明确需要定期备份的重要业务信息、系统数据及软件程序等；
e) 应采取安全防护措施，保护备份信息的保密性、完整性和可用性；
f) 应将重要操作系统和业务系统的备份信息存储在隔离设备或者没有配置操作软件的存储器中；
g) 对需要采取加密或数据脱敏处理的备份数据，进行备份和加密操作时要求两名工作人员在场；
h) 应建立异地备份策略，异地备份存储场所的物理环境安全要求应与系统本地相同；
i) 应对异地备份存储设备进行适当配置，确保其能够及时有效的执行恢复操作。

5.5.13 维护维修管理

本项要求包括：

a) 应制定工业控制系统日常巡检管理制度，明确巡查要点，关注安全设备的日志记录，及时发现异常情况；
b) 应结合设备状态，制定纠正性维修策略和预防性维修策略，并结合核电机组大修做好工业控制系统预防性维护，保障安全；
c) 所有的维护维修工作均应编制相应的技术规程，清楚地列出所执行的操作，避免不当操作对系统运行带来风险；
d) 应制定维修阶段外部人员网络安全管理制度，并按制度严格执行；
e) 应制定维修阶段外接设备、移动存储介质的管理要求；
f) 不应将外部人员携带未经审核检查的移动存储介质、外接设备等接入工业控制系统。

5.5.14 业务连续性保障

本项要求包括：

a) 应制定核电厂工业控制系统业务连续性的设计规划，识别进行连续性规划时所面临的风险以及如何消除这些威胁；
b) 应定期对业务连续性规划进行验证，若发现不足或有缺陷的地方，应及时修订。

5.5.15 设备报废

本项要求包括：

a) 工业控制系统设备和存储介质报废前应使用恢复出厂设置、格式化、消磁等方式清除设备的配置信息和介质内存储的业务数据，并确认配置信息、数据已清除；
b) 应用于工业控制系统的移动存储介质、设备在报废时应执行物理销毁；
c) 涉及报废审批、执行流程应由业务归口部门和安全监督部门共同参与，并做好记录备案。

5.6 退役阶段管理要求

5.6.1 制度管理

本项要求包括：

a) 核电厂工业控制系统的网络安全管理制度应包含工业控制系统设施退役和人员离岗相关的管理规定；
b) 在核电厂退役过程中，应建立网络安全管理制度，对信息的转移或销毁等进行规范化管理。

5.6.2 风险评估

本项要求包括：

a) 应对退役工业控制系统进行评估，重点考虑被退役的硬件和软件的网络安全要求；
b) 退役过程应重点考虑退役系统的保密性要求，确保敏感信息不会泄露；
c) 应对系统退役后的残余风险进行评估，确保残余风险是在电厂的可接受范围内。

5.6.3 设备管理

本项要求包括：

a) 应建立与保护对象相关的设备清单，明确资产管理的责任人员或责任部门，并对资产的转移和销毁等进行规范化管理；
b) 应对核电厂工业控制系统退役的部分进行分析，包括历史数据、硬件、软件，或者整个系统；
c) 对退役报废的系统和设备应按相关要求，销毁含敏感信息的介质和重要安全设备；
d) 应对退役设备执行报废流程，在对服务器、终端、网络设备采取相应网络安全措施后报废设备；
e) 应对载有敏感信息的媒体加以安全妥当的保存或采用安全的方式加以处置；
f) 应对包含存储介质的退役设备进行全面核查，以确保在处置之前，任何敏感信息和注册软件已被删除。具体可进行物理销毁，或采用使原始信息不可获取的技术进行破坏、删除或写覆盖，不得采用一般的删除或格式化处理；
g) 应对退役设备的处置进行记录，以便保持审核记录；应指定专门的部门或人员定期对资产的变动情况进行审核。

6 核电厂工业控制系统网络安全技术防护

6.1 防护总体要求和纵深防御原则

核电厂工业控制系统的防护总体原则应遵循国家网络安全等级保护和电力监控系统网络安全防护的原则。

核电厂应建立工业控制系统网络安全纵深防御模型，根据系统的重要性划分安全防护等级，并为不同等级的系统制定相应的防护措施，各层防护措施的有效性应保持连续且相对独立。安全重要的工业控制系统应处于防御模型的最严等级。核电厂网络安全防护等级的说明见附录A。

6.2 系统安全防护基本要求

6.2.1 物理安全防护

本项要求包括：

a) 核电厂工业控制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；
b) 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；
c) 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；
d) 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。

6.2.2 分区分域及边界防护

本项要求包括：

a) 电厂生产控制大区与管理信息大区之间的通信必须部署经国家主管部门检测认证的专用单向安全隔离装置；
b) 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电力专用横向单向隔离装置；

c) 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；

d) 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；

e) 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，且不影响工业控制系统数据传输的响应要求；

f) 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。

6.2.3 通信网络安全

本项要求包括：

a) 核电厂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；

b) 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；

c) 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；

d) 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；

e) 应及时清理网络设备、安全设备上临时用户、多余用户；

f) 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；

g) 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。

6.2.4 计算环境安全

本项要求包括：

a) 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；

b) 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；

c) 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；

d) 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；

e) 生产控制大区内应部署安全审计设备，能够对操作系统、数据库、业务应用的重要操作进行记录、分析；

f) 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；

g) 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；

h) 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；

i) 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；

j) 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；

k） 宜采用自主可控的安全增强系统实现以上要求。

6.2.5 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可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。

6.2.6 集中管控

本项要求包括：

a） 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；
b） 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；
c） 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；
d） 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；
e） 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；
f） 应能对网络中发生的各类安全事件进行识别、报警和分析；
g） 应在专用场所建立集中的监控中心；
h） 应独立实行系统管理、审计管理和安全管理。

6.3 核安全功能与网络安全功能的协同

6.3.1 核安全功能与网络安全功能原则要求

核电厂工业控制系统的网络安全措施的实现不应影响核安全功能的实现，需要考虑对工业控制系统的网络失效模式和失效后果影响，对工业控制系统的性能（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。

6.3.2 工业控制系统网络安全应急与核安全应急协调机制

本项要求包括：

a） 应将工业控制系统网络安全应急响应纳入应急管理体系中进行统一管理；
b） 核电厂的工业控制系统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。

7 核电厂工业控制系统网络安全应急管理

7.1 应急管理体系

7.1.1 制度和规程

核电厂运营单位应将工业控制系统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） 应建立工业控制系统网络安全应急响应的组织，组织的负责人应为电厂生产运维领域或工业控制网络安全领域第一负责人；
b） 工业控制系统的运维工程师、核安全工程师和其他运行及支持人员应参与应急组织；
c） 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工业控制系统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。

7.1.2 审核和更新

本项要求包括：

a) 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；

b) 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；

c) 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；

d) 应定期对过去的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。

7.1.3 培训和宣贯

本项要求包括：

a) 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；

b) 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；

c) 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；

d) 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；

e) 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。

7.2 安全事件管理

7.2.1 安全事件监测

本项要求包括：

a) 应对系统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；

b) 应监控工业控制系统网络安全边界，以确保及时发现存在潜在的安全威胁并采取相应的措施；

c) 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；

d) 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。

7.2.2 安全事件上报

本项要求包括：

a) 针对系统中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；

b) 应定期组织网络安全机构与工业控制系统运行部门间关于系统网络安全事件的沟通交流；

c) 当工业控制系统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，应按照有关规定向相应的主管部门汇报。

7.2.3 安全事件处置

本项要求包括：

a) 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；
b) 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；
c) 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；
d) 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；
e) 应通过对网络安全事件的评价分析，获取的网络安全事件的特征经验，用于识别易重发的或高安全风险的事件，并采取必要措施避免类似事件重发。

7.2.4 安全事件恢复

本项要求包括：

a) 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；
b) 应确保系统恢复后，系统运行状态与事件发生前一致；
c) 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。

7.3 应急响应

7.3.1 协调和保障

本项要求包括：

a) 应从人力、设备、技术和财务等方面确保应急响应工作的执行有足够的资源保障；
b) 应成立应急响应小组，并明确规定小组成员的岗位职责，负责对全厂工业控制系统安全事件进行响应；
c) 应与各外部支持单位建立密切协作关系，确保支持单位了解应急响应工作和责任；
d) 应协调应急响应工作相关计划和活动与其他工作计划和活动之间的协调性和一致性。

7.3.2 应急演练

本项要求包括：

a) 应制定相应的应急响预案、现场处置方案，并根据计划对应急预案进行演练；
b) 核电厂运营单位应定期组织工业控制系统网络安全(不超过12个月至少进行一次)应急演练，包括应急组织的协调演练和应急处理程序的演练；
c) 应急组织的演练以面向工业控制系统的故障或网络安全攻击为目标，应急响应组织负责人作为演练的负责人，各个相关部门参与，以确保应急组织的总体有效运作；
d) 应针对系统、组织机构或应急预案发生变更时，对应急预案进行演练；
e) 应在实验室、测试平台进行应急演练，模拟评估应急处置能力；
f) 应急演练后，应组织对应急预案的审核和讨论会议，根据演练结果，对应急预案及应急管理程序进行修订完善；
g) 核电厂应编制工业控制系统网络安全事件应急预案，并根据应急演练反馈或发生重大变化时对应急预案及时进行修订。

7.4 网络安全应急与核安全应急协同

本项要求包括：

a） 应建立工业控制系统网络安全应急与核安全应急协调机制；

b） 应判断工业控制系统网络安事件是否导致核安全事件发生；

c） 应急过程中导致核安全事件发生，应统一进行应急指挥调度。

附 录 A
（资料性）
核电厂工业控制系统网络安全定级说明

针对核电厂工业控制系统，应根据对系统成功进行网络攻击所造成的对电厂安全和发电影响的最大后果，分配系统的网络安全设防等级。应从功能角度考虑系统，考虑其可能对电厂安全及发电所产生的直接或间接影响，并根据系统实施的最敏感的功能（即被恶意操纵或中断时产生的影响最为严重的功能）来分配该系统的网络安全设防等级。如果系统与网络安全设防等级更高级别的系统存在连接或接口，并且本系统遭受网络安全攻击会对高级别系统实现其功能产生不利影响，那么可为该系统分配更为严格的网络安全设防等级。

核电厂工业控制系统网络安全设防等级由 1 级（需最少保护）至 5 级（需最多保护）构成。

网络安全 5 级和 4 级的系统或设备受到损坏后，可能会使电厂安全受损，导致不同程度的辐射防护屏障失效，造成放射性物质向外释放，因此有可能对公众健康和安全造成不利影响。例如执行保护功能、核安全有关功能的系统：

——保护功能：反应堆保护系统；

——核安全有关功能：过程控制的仪控系统、主控制室的操作和监视系统以及报警系统等。

其中执行保护功能的系统属于网络安全 5 级，其他系统属于网络安全 4 级。

网络安全 3 级用于构建隔离缓冲网络，与网络安全 4 级系统存在通信接口，但是实施了单向隔离，例如设置了隔离装置的通信接口系统。

网络安全 2 级为一般工业系统或生产管理系统，此类系统受到损坏后，可能对电厂正常运行和控制造成损害，中断系统的正常运行，造成设备损坏等，但不会造成放射性物质向外释放。例如模拟机系统、外围就地控制系统等。

网络安全 1 级系统对于技术控制或运行目的没有直接重要性，主要为电厂信息管理系统，此类系统受到损坏后，可能对核电厂运营单位的合法利益造成损害，如造成电厂信息的泄露，使电厂日常运行变得更加困难，增加行政负担等。例如办公自动化系统，行政档案管理系统等。

核电厂应建立工业控制系统网络安全纵深防御架构，建立严格的通信边界，在边界上采取防御措施，评估、保护、预防、监测和缓解网络攻击，并在受到攻击后恢复系统。防御架构模型应采用网络安全设防措施逐层增强的防御层，实现多层边界防护的独立性和多样性，防止他人通过多层网络中相同或相似的安全漏洞，非法访问或控制系统和设备。

图 A.1 给出了一种核电厂工业控制系统网络安全防御模型。

表 A.1 给出了一种核电厂工业控制系统网络安全设防等级划分原则。

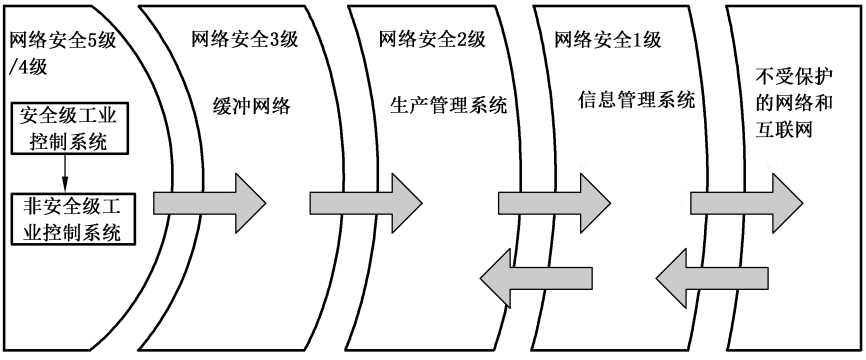

图 A.1 核电厂工业控制系统网络安全防御模型

表 A.1　核电厂工业控制系统网络安全设防等级示例

网络安全设防等级	要求	典型系统
5 级	等级保护 3 级及以上 遵照《工业控制系统信息安全防护指南》 参照 GB/T 33009.1—2016	反应堆保护系统
4 级	等级保护 3 级及以上 遵照《工业控制系统信息安全防护指南》 参照 GB/T 33009.1—2016	过程控制的仪控系统、主控制室的操作和监视系统以及报警系统等
3 级	等级保护 2 级以上 遵照《工业控制系统信息安全防护指南》	通信缓冲网络
2 级	等级保护 2 级	模拟机系统、外围就地控制系统
1 级	商业级信息安全，由核电厂业主确定保护程度	办公自动化系统，行政档案管理系统等

参 考 文 献

[1] GB/T 15474—2010 核电厂安全重要仪表和控制功能分类

[2] GB/T 17901.1—2020 信息技术 安全技术 密钥管理 第1部分:框架

[3] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[4] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[5] GB/T 25069—2010 信息安全技术 术语

[6] GB/T 25070—2019 信息安全技术 网络安全等级保护设计技术要求

[7] GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

[8] GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

[9] GB/T 33009.1—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分:防护要求

[10] GB/T 33009.2—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第2部分:管理要求

[11] GB/T 33009.3—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第3部分:评估指南

[12] GB/T 33009.4—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第4部分:风险与脆弱性检测要求

[13] GB/T 36572—2018 电力监控系统网络安全防护导则

[14] NB/T 20428—2017 核电厂仪表和控制系统计算机安全防范总体要求

[15] ISO/IEC 9798 Information technology—Security techniques—Entity authentication

[16] IEC TS 62443-1-1:2009 Industrial communication networks—Network and system security—Part 1-1:Terminology, concepts and models

[17] IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1:Establishing an industrial automation and control system security program

[18] IEC 62443-3-2:2020 Security for industrial automation and control systems—Part 3-2:Security risk assessment for system design

[19] IEC 62443-4-1:2018 Security for industrial automation and control systems—Part 4-1:Secure product development lifecycle requirements

[20] IEC 62443-4-2:2019 Security for industrial automation and control systems—Part 4-2:Technical security requirements for IACS components

[21] IEC 62645:2019 Nuclear power plants—Instrumentation, control and electrical power systems—Cybersecurity requirements

[22] IEC 62859:2016+AMD1:2019 Nuclear power plants—Instrumentation and control systems—Requirements for coordinating safety and cybersecurity

[23] IAEA Nuclear Security Series No. 17:2011 Reference Manual, Computer Security at Nuclear Facilities

[24] IAEA 安全标准丛书 No.SSG-39 核电厂仪表与控制系统设计

[25] HAD 102/14 核电厂安全有关仪表和控制系统

[26] 发改能源〔2018〕765号 关于进一步加强核电运行安全管理的指导意见

[27] 工信部信软〔2017〕188号 工业控制系统信息安全防护能力评估工作管理办法

[28] 工信部信软〔2016〕338号 工业控制系统信息安全防护指南

[29] 国能安全〔2015〕36号 附件1:电力监控系统安全防护总体方案

[30] 国家发展改革委员会2014年第14号令 电力监控系统安全防护规定