

ICS 27.120.20

F 69

备案号: 38337-2013

NB

中 华 人 民 共 和 国 能 源 行 业 标 准

NB/T 20147—2012

核电厂实物保护系统设备准则

Criteria for physical protection systems for nuclear power plants

2012-10-19 发布

2013-03-01 实施

国家能源局 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 集成化安保系统..... 3

5 周界入侵报警系统..... 7

6 安保照明系统..... 9

7 视频监控系统.....11

8 出入口控制系统..... 13

9 室内入侵报警系统..... 15

10 数据采集、处理和显示系统..... 16

11 安保通信系统..... 20

12 线路监视..... 21

13 胁迫报警..... 22

14 安保供电系统..... 22

15 维护及测试..... 24

前 言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替EJ/T 571—1991《核电厂保卫系统电气设备准则》，与EJ/T 571—1991相比，除编辑性修改外主要技术变化如下：

- 增加了“集成化安保系统”（见第4章）；
- 增加了术语“实物保护、出入口控制、探知、报警、证件号码、实体屏障、读卡器、信息安全、误报警、噪扰报警、要害区、重要设备”等（见3.1、3.3～3.8、3.10、3.14、3.17、3.23、3.24）；
- 修改了安保照明系统的技术要求和技术参数（见6.2.1～6.2.3、6.3.2、6.4.2，1991版的4.2.2.1.1、4.3.2.1、4.4.2.1）；
- 修改了视频监控系统的技术要求和技术参数（见7.2.2，1991版的9.4.3）；
- 修改了出入口控制系统的技术要求和技术参数（见8.3.3，1991版的7.3.3.1），增加了出入口管理中对违禁物品探测的措施要求（见8.3.5～8.3.7）；
- 修改了数据采集、处理和显示系统的技术要求和技术参数（见10.2、10.3.2，1991版的12.2～12.4）；
- 修改了线路监视的技术要求和技术参数（见10.2、10.3.2，1991版的8.2）；
- 增加了对信息安全的要求（见4.3.9）。

本标准由能源行业核电标准化技术委员会提出。

本标准由核工业标准化研究所归口。

本标准起草单位：中国核电工程有限公司。

本标准主要起草人：丁燕、郭璇、范君龙、王晓宇、郭韶华、张丽霞、杨霞、汪永忠、丁大弼、李征、王劲。

EJ/T 571于1991年10月首次发布，本次为第一次修订。

核电厂实物保护系统设备准则

1 范围

本标准给出了核电厂实物保护系统设备的设计、测试和维护技术准则。

本标准适用于核电厂保卫力量针对核安保威胁所采用的永久或临时安装的系统、子系统和部件。它包括核安保相关的探测、复核、监视、出入口控制、通信和数据采集设备。

本标准还适用于探测、监视、显示及记录核安保事件和环境情况的相关设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

实物保护 physical protection

为防止入侵者盗窃、抢劫或非法转移核材料或破坏核设施所采用的保护措施。

3.2

实物保护系统 physical protection system

采用探测、延迟及反应的技术和能力，阻止破坏核设施行为和防止盗窃、抢劫或非法转移核材料活动的安全防范系统。

3.3

出入口控制 access control

作为出入口控制系统的一部分，对人员企图进入控制区域的授权和访问权限进行核查。

3.4

探知 acknowledge

值班人员表示知道发生报警或某事件的行为。

3.5

报警 alarm

探测器或探测系统发出的报警，通常以声或光信号发出；该信号可能是误报警、噪扰报警或有效报警。

3.6

证件号码 badge number

分配给通行证件的一组数字特征编码。

3.7

实体屏障 physical barrier

栅栏、围墙或类似的障碍物。可以起到入侵延迟的作用和协助出入口控制的作用。

3.8

读卡器 card reader

设在出入口，用于读取带有授权资格信息编码的设备。

3.9

保卫控制中心 central alarm station

连续24小时值班，作为监控实物保护系统运行的主要场所，为要害区。

3.10

信息安全 cyber security

计算机系统、软件程序或重要内部模块，以防止企图通过互联网、公共或专用通信网用非法手段或误操作来干扰、损害计算机系统或使系统失效所具有的能力或薄弱性。

3.11

探测区域 detection zone

探测器能够探测入侵行为的区域。

3.12

胁迫报警 duress alarm

当核电厂员工被挟持进行不良行为时发出的报警信号。

3.13

事件 event

状态或条件的变化。

3.14

误报警 false alarm

由于设备的本身故障引起的报警。

3. 15

入侵报警 intrusion alarm

具有非法行为指示功能的电气、电子、光电、机电或类似设备，用于探测人员进入建筑物、保护区、要害区域或核材料使用区域的入侵行为，并通过声光信号向警卫或保卫人员发出报警。

3. 16

隔离带 isolation zone

实体屏障双层围栏之间的特定地带，其内部没有能隐藏或掩蔽人体的物体。

3. 17

噪扰报警 nuisance alarm

并非由于人员入侵但确因有一触发信号触发探测器而引起的报警。

3. 18

巡逻 patrol tour

保卫人员沿预定路线观察沿途区域的安保情况所进行的巡查。

3. 19

保卫区域 protected area (PA)

由实体屏障围成的、控制出入的区域。

3. 20

保卫 safeguard

对核电厂的核材料和重要设备所采取的实物保护措施。

3. 21

安保系统 security system

一组硬件和相关软件的集合体，包括核电厂实物保护以防止造成放射性破坏的设计基准威胁所必需的所有部件、设备和屏障等。

3. 22

篡改 tamper

干扰或损坏数据有效性或装备完整性的行为。由此使实物保护系统原有功能受到威胁、影响或不能正常发挥。

3. 23

要害区 vital area

处于保护区内，设有重要设备、系统或装置，或存有核材料的区域。该区域内的保护对象遭到破坏，可能直接或间接导致不可接受的放射性后果。

3.24

重要设备 vital equipment

重要设备是指相关设备、系统、装置或材料，其失效或被破坏，可能产生直接或间接的危及公众健康和安全的放射性释放后果。另外在上述失效或被破坏的情况下，用于保护公众健康和安全的系统和设备也应视为重要设备。

4 集成化安保系统

4.1 设计原则

实物保护系统是集成化安保系统，本章规定了集成化安保系统的总体要求和设备接口。组成实物保护系统的各种不同类型的设备（或子系统）的详细要求见第5章～第15章。

集成化安保系统是用于支持核电厂实物保护系统的电子系统，具备抵御设计基准威胁的能力，可防止放射性释放破坏的企图，以保护社会公众健康安全。

集成化安保系统应能探测并将核电厂实物保护面临的威胁通知保卫人员。

集成化安保系统应具备设施保卫程序中所要求的功能，即在保卫控制中心采集、显示系统产生的报警或异常情况、并发出声光报警。集成化安保系统应通过视频监控或其他合适的手段观察和复核周界隔离区和实体屏障的情况。集成化安保系统还应为出入口控制、应急通道管理和反应力量通信提供设备。

为了保证核电厂实物保护系统各子系统的有效配合，集成化安保系统应统一授时，保证各子系统具有相同的时间基准。

核电厂实物保护系统应根据相关文件进行建造、设计、生产、施工和运行，这些文件提出了集成化安保系统的各子系统及组件的设计基准和要求。室内和室外的安保设备应具有防雷击和防浪涌保护措施，使设备的失效或故障率降至最小。

4.2 实物保护系统子系统和设备的组成

集成化安保系统应包括（但不限于）以下各系统（或子系统）：

- a) 周界入侵报警系统；
- b) 安保照明系统；
- c) 视频监控和报警复核系统；
- d) 出入口控制系统；
- e) 室内入侵报警系统；
- f) 数据采集、处理和显示系统；
- g) 安保通信系统；
- h) 线路监视；
- i) 胁迫报警；
- j) 供电系统等。

集成化安保系统还包括设备连接电缆、电缆敷设通道和防雷接地设备等，应考虑设备的维修和测试要求。

4.3 总的性能要求

4.3.1 集成化安保系统接口

实物保护系统设备（或子系统）之间的典型接口布置见图1。



图1 集成化保安系统接口

4.3.2 结构控制

集成化安保系统的软件和硬件应根据相关设计控制文件来维护,以保证集成化安保系统的设计未经正式的批准不应改变。

4.3.3 实物保护要素（组成部分）

实物保护系统保护目标的确定和实物保护系统针对各目标的适应性分析不在本标准的范围内,但属于核安保的重要相关要素。实物保护要素间的关系及本标准包括内容的示意图见图2。



图2 实物保护要素

4.3.4 实物保护分区

实物保护设计包括在全厂设置多个实物保护分区。图3是一个典型的实物保护分区和特征的示意图。典型的实物保护系统设计还包括利用屏障来防止恶意使用车辆非法闯入核电厂。

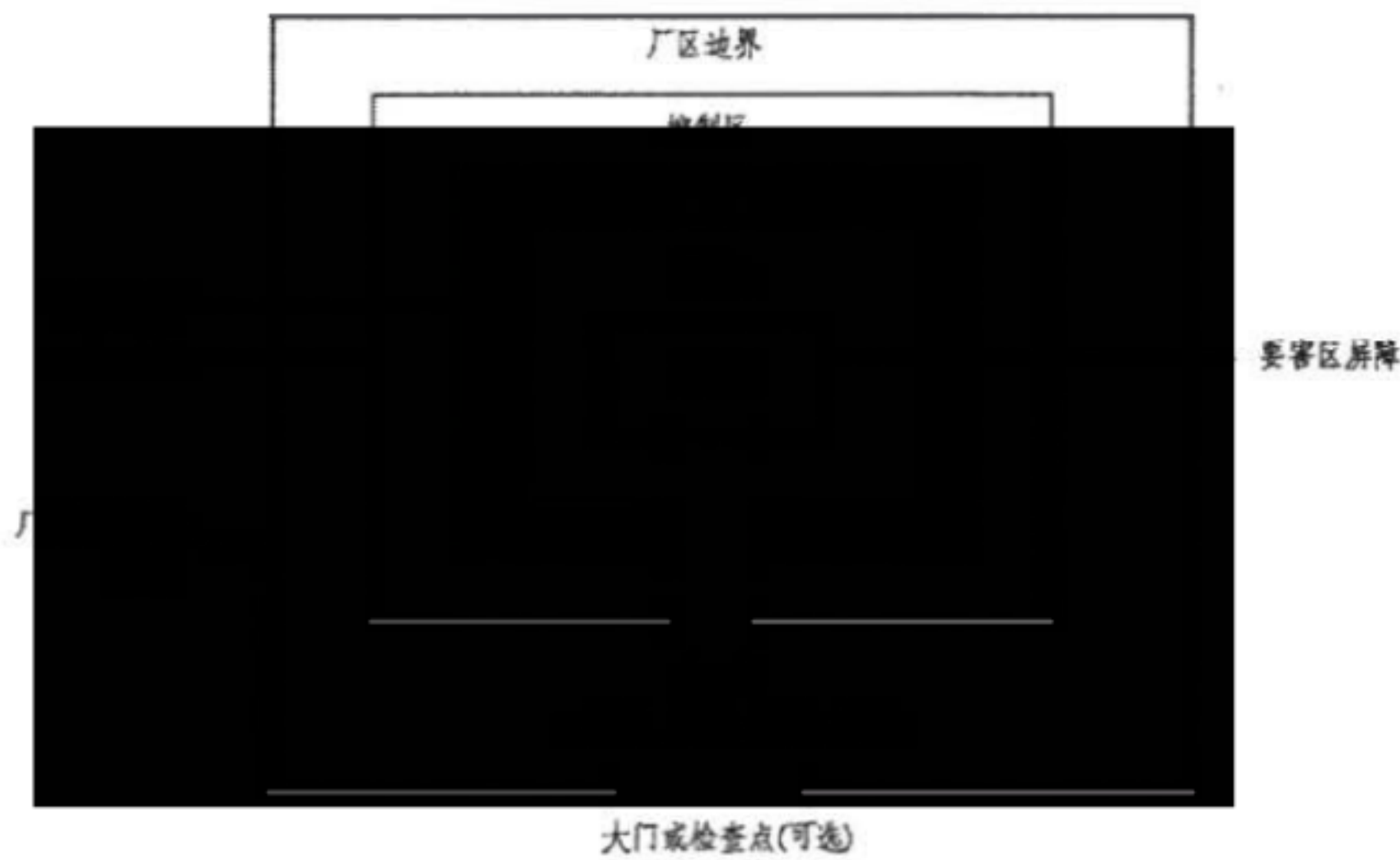


图3 典型的实物保护分区

4.3.5 防篡改保护

探测器和装有安保设备的箱体上应装有防篡改开关或其他触发装置。这些防篡改设备在探测到设计要求的外部触发行为或条件时，发出防篡改报警信号。

4.3.6 性能的设计验证

独立的实物保护系统验证要求如下：

- 工程和设计验证应独立于原设计者；
- 系统、设备或部件的制造和施工的人员不应直接参与测试标准的制订、审查和批准；
- 系统、设备或部件的制造和施工人员不应直接参与实物保护系统的测试验证；
- 该系统、设备或部件的制造和施工的人员不应直接参与审核测试结果。

此类测试应满足子系统或部件规格书的要求。

在发货前应进行厂内测试以验证系统的功能完好。集成系统安装后应由该集成系统制造和施工以外的人员进行测试并验证以满足集成系统的技术性能要求。验证应在集成系统投入运行前完成。除非另行规定，子系统应按照生产厂家的建议来运行、测试、维护。除非另行规定，子系统或部件的修改应与原系统的设计要求和设计验证等级相一致。

4.3.7 设计基准文件

至少应编制并提供包括以下信息的文件，可有效地用于准备实物保护系统的运行操作程序、设计出入口控制和相关的探测硬件：

- a) 威胁评估，实物保护系统设计基准文件应包括对假定的破坏、入侵者威胁的明确描述；
- b) 目标的列表，根据假设的威胁、核电厂的实际布置、出入口控制流程，应进行分析以确保核材料、设备和区域得到保护，防止破坏活动得逞。威胁分析应形成一份含应得到保护的核材料、区域和设备的列表；
- c) 出入口控制和探测设计方案，出入口控制和探测设计方案应确定允许人员、包裹、货物和车辆合法进出保卫区域的方式和特点。这些方式 and 特点应包括针对非法携带核材料或违禁品的检查手段、探测和报警的手段及对通道门、旋转栅门、检查通道等出入口的管理要求等；
- d) 运行管理程序，实物保护系统设计应贯彻于硬件设备和运行管理程序，用于保护区和要害区合法通行。这些程序的制定应基于假定的威胁、重要的设备，以及在正常工况、异常工况和应急工况下合法出入保护区和要害区的需求。

4.3.8 质量保证

核电厂安全相关设备质量保证准则的要求不适用于核电厂实物保护系统。

4.3.9 信息安全措施

信息安全应作为实物保护系统要求的一部分。数字计算机、通信系统、与实物保护系统相关的网络应采用独立专网，并在设计和运行时确保具有足够的保护措施，以应对信息攻击的行为，否则可能对以下方面产生不利影响：

- 数据和（或）软件的完整性和机密性；
- 系统、服务器和（或）数据的访问；
- 系统、网络和相关设备的运行。

实物保护系统专网的防护等级宜按照信息系统安全等级的三级防护等级进行保护，具体要求应符合 GB/T 22240—2008 和 GB/T 22239—2008 的要求。

5 周界入侵报警系统

5.1 设计原则

周界入侵探测系统的设计目的是探测到体重超过35 kg的入侵者，无论该入侵者以跑、走、爬、跳或滚的方式穿过周界探测区域。应限制系统的误报警率和噪扰报警的总数。在保证探测概率的同时，每个探测段的噪扰报警或误报警每天不应超过1次。

周界入侵探测系统的设计应考虑到现场的地形地貌、现场环境因素、性能要求和安全保障。周界入侵探测系统用来探测入侵者穿过屏障之前的企图和实际穿越保护区域的周界屏障的行为（包含经过任何易被忽视的且可能通过的路径）。周界入侵探测系统设计应满足以下要求：

- a) 探测系统设置在被保护区域屏障的外侧一段距离之内，使安保机构（反应部队）有足够的反应时间；
- b) 在保卫控制中心内显示报警；
- c) 有效地探测设计基准威胁界定的一个或多个的入侵者；
- d) 利用各种探测方法使入侵者无法躲过探测。

5.2 周界入侵探测系统探测器的类型

以下为几种常用的周界入侵探测器，但并不仅限于此：

- a) 微波报警系统；
- b) 静电场报警系统；
- c) 主动红外报警系统；
- d) 开口同轴电缆报警系统（泄漏电缆）；
- e) 视频移动探测系统；
- f) 缆式振动探测器；
- g) 栅栏防破坏探测器等。

应根据现场的地形地貌、环境因素、性能要求和安全保障要求来选择合适的探测器，具体要求详见5.3～5.7。

5.3 现场评估、系统选择和安装

应根据全面的现场评估来选择合适的周界入侵报警系统探测器。影响周界入侵报警系统的现场环境包括但不限于以下内容：

- a) 地形——周界入侵探测系统应位于或设在地形特征对探测和复核影响最小的地方。应根据地形特征确定探测器的灵敏度。在选择周界探测器时，应考虑以下几方面的环境因素：
 - 1) 陡坡；
 - 2) 沟壑或沟渠；
 - 3) 水道；
 - 4) 水面。
- b) 植被——应减少植被引发的探测器性能降低或噪扰报警；
- c) 野生动物——应考虑野生动物的潜在不利影响。动物会引发噪扰报警和损坏探测器。可以用围栏进行隔离和驱除的方式来控制野生动物对系统的影响；
- d) 背景噪声——应考虑背景噪声的多样性。应选择适当的探测器种类，使其不受背景噪声影响而降低性能；
- e) 气候和天气——在选择、布置及安装电气设备时应考虑气候和天气因素（包括：雨、冰雹、风、雪、雾）。在选择探测器时应关注：设备的防护等级、设备的内部构造及温度等级。应根据环境需要考虑设备配备加热和（或）冷却装置；
- f) 土壤和铺设的地面——土壤和铺设的地面应考虑满足探测器的运行要求，且将噪扰报警降至最低。雨水飞溅、反弹落石、积水洼地均可能产生噪扰报警；

- g) 交通情况(空中和地面)——探测器的选择和布置应考虑交通情况和地表震动的影响,将噪扰报警降至最低。交通工具引起的电磁背景噪声、车辆的经过可能会引起的水滴和碎石的飞溅等均可能引发噪扰报警;
- h) 保护区域的大小和位置——保护区域的大小和位置会影响探测器的数量、安保系统的规模、最终安装费用、运行中的维护和更新。保护区域的大小和位置应便于设备运行、现场测试以及现场维护,并符合厂址的客观情况;
- i) 盐雾——在探测器的选择、布置和电器元件安装时应考虑到现场的盐雾环境影响。根据现场的盐雾环境确定适当的设备外壳防护和设备内部构造;
- j) 电磁场和高压线场所——应尽量减少电磁场的电气噪声影响。应选择或保护探测器,使其不因电气噪声而降低性能。电气噪声源包括架空电力电缆、变压器、移动电话、手持无线电通信设备等。高压线会产生电磁背景噪声使安保探测设备产生误报警;
- k) 光照角度——阳光照在红外报警器上可能导致探测器不能正常工作;
- l) 厂区系统/设备的排放物和释放物——加热、制冷或排气系统所产生的温度快速变化会影响某些探测器的正常工作,例如微波探测器和红外探测器。

5.4 布置

室外探测器的布置应最大限度地发挥探测能力,同时将噪扰报警和误报警率降至最低。探测器宜尽可能布置于双层屏障之间(一般,外侧屏障用于减少噪扰报警,内侧屏障用于增加延迟)。探测器应该设置在一定高度和离开屏障一段距离,以防止入侵者利用屏障或通过搭桥的方式翻过屏障或绕过探测。

应将周界分成若干探测段,在每个探测段设置探测设备,探测段布防区域应连续,相邻探测段间不应存在探测盲区。探测段的长度应受限于以下两点:

- a) 探测器的最佳性能(以探测概率、误报率和噪扰报警率为标准);
- b) 应便于对探测段全面观察以达到有效复核的目的。复核可通过人员现场确认和视频监控手段实现。

5.5 探测概率

周界入侵探测器的选择和布置应使系统的探测概率符合如下要求:

- a) 每个探测段对入侵的探测概率在95%的置信水平下不低于90%;
- b) 对探测器要进行定期测试以确保探测区域和每个区域的探测概率;
- c) 体重大于35 kg的入侵者以0.15 m/s~5 m/s之间的速度穿过探测区域应被探测到。

在正常环境条件下,整个周界报警系统在维持适当的探测灵敏度时,每个探测段或每个报警点每周平均误报警不宜超过一次,并且每个探测段或每个报警点每周噪扰报警不超过一次。由一个暂时事件引起的多种误报警、噪扰报警或两者兼有,应被视为单次报警。为了保证在各种环境下都达到90%以上的探测概率,减少噪扰报警,可选探测机理不同而性能互补的探测器。在人员或视频监控始终能观察到的区域,误报警率和噪扰报警率可增加到每天每个探测段或每个报警点一次。

每个季度要分析和确定平均报警率的趋势。

5.6 必需的报警条件

周界入侵报警系统在探测到符合5.1的设计原则的入侵行为时,应发出一个报警信号。

5.7 防篡改保护

对于没有自保护功能的或者没有位于任一探测器探测区域内的探测设备和相关设备箱体,应设置防拆开关或其他触发报警装置。

6 安保照明系统

6.1 设计原则

安保照明系统应为监视及观察目标提供足够的照度,以便能对入侵者做出判断,并采取必要的措施。照度水平应满足视频监控系统或人员直接观察的要求。

安保照明系统应为巡逻人员、反应部队和具有低照度功能的视频设备提供能够满足探测、监视、追踪及响应要求的照明。

本章节的设计安装标准仅适用于安保照明。安保照明系统可以是一个独立的专用系统,也可纳入能满足安保照明系统条件的全厂室外照明系统。

安保照明系统应为监视、威胁评估、设施安保力量抓捕入侵者提供保障。

6.2 室外安保照明

6.2.1 室外照明的总体要求

室外安保照明应为隔离带和保护区域的所有室外区域提供照明。室外区域包括高度在5.4 m以下的区域和高度大于等于5.4 m并且在那里设有上下无防护的通道(如直爬梯、电缆竖井、管道等)的区域。照明的强度、均匀度、显色性应保障保卫人员通过视频监视或直接观察保护区域。不应产生能藏身的阴影,也不应产生影响保卫人员观察的眩光。

6.2.2 照度

室外安保照明设备在其寿期内应为保卫人员通过视频监视或人员直接观察提供足够的照度。

此外,室外安保照明系统应提供足够的照度,以保障保卫人员在夜里可观察到100 m范围内1.5 m高,23 cm宽的人及其所做的动作,动作是指:躺卧、匍匐前行、站立、行走、奔跑等;并保障保卫人员能够不用辅助照明完成保护区域内周界巡逻任务。室外安保照明应有足够的照度水平,使视频监控系统能够清晰显示监视区域。保护区隔离带的地面水平照度应不小于20 lx。

6.2.3 照明均匀度等级

地面的水平照度不宜低于平均照度的1/5。当视频监视用于监视和报警复核时,为了保证摄像机的最佳运行,每个监视区域宜采用一致的照度标准和统一的照明设备。

6.2.4 光源

光源色温及光谱的选择应与视频监控系统的要求相一致。

6.2.5 照明可靠性

安保照明的可靠性分析应在基准威胁的基础上进行。

6.2.6 照明控制

室外安保照明应能自动开启或关闭。在自动控制故障或因其他原因中断时,应能手动控制灯具的开或关。手动控制开关应设置在保卫控制中心或某一重要地点。

6.2.7 供电中断

室外安保照明系统电源的中断不应影响报警复核功能的实现。光源在整个寿期内应维护保养以保持足够的照度。应采取措施防止隔离区内所有照明丧失的情况发生。安保照明应考虑备用电源供电。

6.2.8 照明构筑物

灯塔、灯柱、灯杆或用来固定支撑这些设备的构筑物应具有适合厂址气候条件的能力。周界照明构筑物的安装位置应考虑防止入侵者借助其避开周界探测。

6.2.9 室外照明老化影响

室外安保照明系统设计应考虑照明随时间正常老化的现象。灯具的光效应取光源在最后一次清洁之前并且是其寿命将至终止时的光效。

6.3 主要出入口安保照明

6.3.1 主出入口总体要求

应为保护区的主人员入口和车辆出入口提供足够的照明以保障视频监视和保卫人员活动能够正常进行。

6.3.2 照度

人员通过的出入口，照度水平宜为150 lx，目的是能够对通行人员的面部进行识别并应把眩光减到最少。

在车辆出入口照度水平不宜低于150 lx。照明设计应能照亮所有进、出车辆的侧面与顶部。保卫人员在对车辆底盘进行检查时可用便携手提式灯具。

6.4 室内安保照明

6.4.1 要求

为使人员直接观察或视频监视，室内的重要区域和通过重要区域的通道应考虑照明设计。

6.4.2 照度

在要求直接目视监视的区域内，宜保持照度不低于20 lx。

视频监控系统所需的区域照明应具有与监视设备相匹配的照度。

6.4.3 应用

灯具类型和安装方式应考虑与所使用区域的环境条件相适应。

7 视频监控系统

7.1 设计原则

应建立适用于保护核电厂的、可防御设计基准威胁的远程视频监控系统。视频监控系统提供了一种远距离监控和评估保护区的手段。视频监控系统应便于对穿越受保护区探测的报警复核和对面临威胁的评估做出初期的反应。

为了便于对穿越保护区的入侵做出初期的反应，并对威胁进行评估，应采用视频监控系统对保护区隔离带和要害区域周界实体屏障进行观察。通过观察周界探测区域，要求在保卫控制中心显示的信息能够有效评估报警的原因和存在的威胁。其他摄像机用于监控保护区周界上各种人员、车辆和货物的出入口。视频监控系统还用于厂区的其他区域内的一般观察。电子监控技术手段和监控计划内的安全人

员管理应用的结合是安全计划成功的必要条件。应根据保卫控制中心人员报警复核的要求确定合适的监视器尺寸、布置以及显示的画面质量。

任一周界报警发生时，周界探测区域显示图像应能使值班人员评估报警的原因和潜在威胁。人员出入口、车辆出入口和警卫检查车辆的显示图像应能使值班人员有效评估警卫可能受到胁迫的状况。

7.2 性能要求

7.2.1 总体性能要求

视频监控系统应每天24 h运行。系统应在正常的（预期的）环境条件下保持可用。在短时发生的异常条件（也就是台风、龙卷风、意外的暴雨、雪暴和冰暴、极端的大风等）可能会降低系统的性能。

视频监控系统应与入侵报警系统、安保照明系统、供电等统的应用相适应。

7.2.2 定焦摄像机覆盖范围

视频监控系统应在保卫控制中心清晰显示周界探测区域、人员和车辆出入口的图像。要求摄像机的观察图像显示的探测区域应没有大到可以隐藏一个人的遮挡物。

摄像机的观察视野受限于距离，超出距离值班人员将无法判别物体的性质。当物体在任何位置移动、站立、平放时，值班人员应能判定这个物体属性，并评估该物体的行为和动作。视频监控系统推荐的最小可接受的分辨率是0.3 m高的物体占不低于观察的水平视野的1%范围，或者相当于一个宽度不大于30 m的场景。

定焦摄像机应能覆盖周界探测区域的整个宽度和长度。应能向值班人员提供发生入侵报警的周界探测区域的实时图像。位于周界探测区域内的建筑物的侧面和顶部或任何其他构筑物应被覆盖到。

定焦摄像机的观察视野应与周界入侵报警系统的探测器位置相互协调，尽量使用不多于两台摄像机就能观察整个探测区域。定焦摄像机宜在周界周围按相同的方向定向布置。

视频监控摄像机的布置还应考虑交通情况。附近道路上车辆的灯光，如果直接照到摄像机可能会干扰摄像机图像，应将这种干扰减到最少。

确定视频监控摄像机的布置时应考虑逆光对摄像机显示图像的影响。较低的阳光入射角度，比如在日出和日落时可能导致摄像机直接面对太阳，会暂时地降低图像质量而影响评估能力。

7.2.3 云台变焦摄像机的覆盖范围

应考虑下列的特征：

- a) 在保护区域内的一些摄像机应配备云台变焦设备来协助检查保护区域的室外区域。分辨率选取宜考虑变焦镜头在其最远处的观察需求；
- b) 视频监控系统应使值班人员清晰观察车辆出入口。宜至少在一台摄像机（每个出入口）上配备云台变焦控制设备并有足够的分辨率供值班人员有效观察。

7.2.4 显示

保卫控制中心应具备视频控制和管理的功能。

应提供对任一摄像机手动的或自动的视频显示进行视频转换，并对任一云台变焦控制装置进行手动的或自动的控制。每一个值班人员应具有全部功能的独立的控制。系统应能在周界入侵传感器发出报警时，同时显示所报警区域的所有摄像机图像。这种自动控制操作应优先于任一个值班人员的操作。

用于报警复核的视频显示应能在值班人员正常岗位前面的专用监视器上进行显示。应根据报警工作站的回放选择监视器的尺寸。监视器的适当的尺寸和位置应确保为值班人员的评估所显示的场景满足7.2.2和7.2.3中所述的要求。

可以选择专用的监视器显示一台摄像机图像,也可将多个摄像机的场景在一台监视器上连续循环显示。在所有循环显示的监视器上的全部场景宜在循环中同时切换。应根据图像复核的人因要求来选择监视器的尺寸。

7.2.5 场景照明

应提供充足的照明以满足视频监控系统一大24h的运行并且图像清晰度不受影响。场景内的各种照明水平不宜影响在监视器上观察到的图像或行动。照明均匀度设计限度是5:1。附加的照度要求见6.2.2。

宜考虑下列的条件和因素(以及相关的照度计算):

- a) 照明应由安保供电系统电源供电;
- b) 灯具寿期末的对照度的影响和灯具表面积尘对照度的影响;
- c) 任一个场景光源的单灯故障对场景照度的影响;
- d) 照明等级与摄像机灵敏度相协调,要求达到完整的视频输出;
- e) 灯具的最低工作电压;
- f) 镜头光圈调节功能停止的影响;
- g) 玻璃的透光率;
- h) 场景的最低照度等级;
- i) 场景内地表植物的反射系数。

7.2.6 摄像机布置

视频监控系统的摄像机的布置设计,可考虑安装在已有建筑构筑物上或专用立杆上。用来支持视频监控摄像机和(或)其他相关设备的杆和构筑物的设计满足核电厂厂址设计文件中所规定的环境条件。立杆的布置应避免被人利用,绕过入侵探测系统。

7.2.7 视频电源

所有视频设备宜从同一单相电源来供电,提供它们之间彼此协调的同步脉冲。

7.2.8 视频的记录与存储

视频录像机、视频存储或其他类型的图像存储系统作为事件回放的手段和工具应有效。宜同时回放每台与周界报警相关的摄像机上的场景。系统宜具有记录或存储满足管理要求时长的视频图像的能力。

7.2.9 时间/日期/区域

所有的视频显示应包含当前时间和日期。所有的视频显示应包括摄像机识别和(或)报警区域编码。显示的信息应足以确定视频场景的地理位置。

7.2.10 信号传输

设计应考虑环境对视频信号传输系统的影响。尤其是当电缆直接在地下管道和管沟内敷设时,应在视频信号传输系统的选型、安装和维护方面考虑以下的影响:

- a) 湿度和水位;
- b) 信号带宽和衰减;
- c) 电导率;
- d) 电磁干扰;
- e) 无线电频率干扰;
- f) 防雷和浪涌保护;

- g) 正常的核电厂辐射水平。

7.2.11 浪涌保护

与摄像机相关的电源、视频、和控制电缆可能常遭受雷击，应通过防浪涌保护装置与视频系统设备隔离。宜采用光纤传输介质传输视频和控制信号。

7.3 设备的防护标准

室外摄像机应选择适合的室外防护罩，以满足厂址现场的环境条件。

7.4 文件

一个完善的监控系统设计文件应包括以下的要求：

- a) 分辨率

按照设计标准中确定的分辨率的要求，针对每个摄像机观察视野范围计算摄像机镜头尺寸和安装高度；

- b) 摄像机的覆盖范围

图纸应表示探测区域的覆盖范围，包括围栏位置和摄像机安装位置；

- c) 摄像机视场范围与入侵探测区域的协调性

图纸应表示摄像机视场范围与周界入侵报警探测区域的关系。

8 出入口控制系统

8.1 设计原则

出入口控制系统的设计原则是控制人员和车辆进出保卫区域所有出入口（当有出入通行请求时）。出入口控制系统应能提供出入通行授权和人员身份识别的手段，具备对个人、车辆和包裹的检查能力。

系统分为两部分：出入控制和检查方法，及操作程序。安保操作程序应与系统硬件设计的特征相适应。出入口控制不应过分妨碍日常运行、测试和维修，同时应满足核电厂运行针对放射性、火灾、厂区失电和安保事件等应急程序的要求。应具备在核应急工况下各出入口控制区域的应急人员清点功能。出入口控制包括以下4个要素：

- a) 限制进出的屏障；
- b) 传输出入通行请求的装置；
- c) 验证授权的装置；
- d) 出入口控制通道装置。

出入口控制和检查的设计方案应说明人员、包裹、货物和车辆合法进出保卫区域的措施。应详细描述检查未经授权携带的核材料和违禁物品的手段和措施、探测和报警手段，对通道门、大门、旋转栅门、检查区域管理手段和技术手段等方面的细节等。

出入口控制系统应具有防返传、防重入、防胁迫功能，提供有效的访客陪访管理手段。

8.2 出入口控制总体要求

8.2.1 出入口控制屏障要求

为防止人员未经许可进入保卫区域，应设置出入口控制屏障。这些屏障可采用电子或机械的手段进行控制。作为限制进入保卫区域屏障的一部分，屏障上的每个门、人孔、入口等电控装置的设计应考虑与设计基准威胁相一致的延迟防护措施。

8.2.2 人员

宜利用金属探测器和爆炸物探测器对进入的人员进行违禁物品检查。

8.2.3 车辆

所有车辆进入保卫区域之前都应进行违禁物品检查。

8.2.4 材料

所有手提式包裹都应通过人员监视观察或检查设备（金属探测器、爆炸物探测器、X-射线装置等）来检查隐藏的轻武器、爆炸物、易燃装置，以及其他可能用于偷盗或破坏目的的物项。

8.3 硬件类型

8.3.1 硬件选择要求

设备的设计需求和布置应满足设计文件要求。出入口控制设备的功能是识别人员的身份，并确认是否具有被授权进出该区域的权限。识别身份的方法应满足误识进入的概率不低于99.9%，同时错误拒绝进入的概率不超过2%。身份验证技术应与环境条件相适合，并为通过通道提供合适的反应时间。出入口控制系统宜考虑8.3.2～8.3.7所描述的出入控制硬件设备。

8.3.2 读卡器及控制器

人员出入卡和读卡器（卡片出入控制系统）用于向出入口控制系统传送个人身份和访问请求信息。读卡器及控制器应满足下列的要求：

- a) 应包含以编码形式存储的身份信息，并能防止读取和复制；
- b) 个人识别码应该在被授权出入人员的范围内随机分配；
- c) 读卡控制设备的设计和安装应考虑将控制设备布置在该出入口防区的内侧、同级别保卫区域或高级别保卫区域内侧，以防止人为破坏；
- d) 设备应防止任何物理形式的袭击，对读卡器的所有破坏都不能引起相连的出入口控制装置开锁；
- e) 设备应具有防篡改保护功能；
- f) 设备应防止操作错误引起出入口控制系统误动作；
- g) 设备应能适应所在环境的影响，具备足够的防护等级和适当的结构设计。

8.3.3 生物识别装置

建议在重要区域的出入口使用生物识别作为确认用户身份的手段。生物识别验证技术的选择应与核电厂的工作环境条件相适合，应考虑尘土、污染物、防护服等工作环境因素。同时在设计选择设备和识别方式时应考虑身份验证时间的要求。

8.3.4 出入口执行装置

出入口执行装置设置于屏障上，其作用为通过出入口控制系统控制人员或车辆进入保卫区域。这些装置包括三角叉门、旋转栅门、车辆防撞液压路障、挡车器、电控门等，应考虑以下因素：

- a) 应在实体屏障的整体设计中考虑；
- b) 出入口执行装置的延迟能力不应成为屏障的薄弱点；
- c) 应具备监控屏障上每个出入口的实际工作情况（开启、关闭、上锁、解锁和篡改）的装置；
- d) 当受到外力强行打开时，应具备自动报警触发的装置（至少在每一重要区域屏障上）；

- e) 在设计中应考虑应急疏散通道的管理需求（推杠锁装置）。

8.3.5 金属探测器

金属探测器用来探测武器和其他金属违禁品。

8.3.6 爆炸物探测器

爆炸物探测器用来探测爆炸物。

8.3.7 X光检查设备

X光机用来探测武器、易燃装置和其他违禁品。

9 室内入侵报警系统

9.1 设计原则

室内入侵探测系统的设计原则是探测非法入侵的人员进入重要区域的行为，应发出报警。入侵报警信号应送至保卫控制中心进行处理。

9.2 描述

9.2.1 出入口传感器

出入口传感器应探测出非法入侵的人员通过通道门进入重要区域的行为。在门被非法打开的情况下，传感器应产生并发出报警。典型的出入口传感器是门磁开关。

9.2.2 其他类型的传感器

其他类型的室内入侵探测传感器包括：

- a) 超声波；
- b) 微波；
- c) 红外线；
- d) 声波；
- e) 电容；
- f) 振动；
- g) 压力；
- h) 视频移动报警；
- i) 玻璃破碎探测等。

选择各种适合的传感器以满足特定场地的探测有效性要求。

9.3 场地评估

应进行全面的场地评估来选择室内入侵探测传感器。应考虑以下影响室内入侵探测系统的场地条件：

- a) 结构布局；
- b) 人员和车辆的交通情况；
- c) 运动中的物体；
- d) 可移动的物体；

- e) 背景噪声;
- f) 环境;
- g) 空气的流动。

9.4 性能要求

9.4.1 布置

传感器位置的选择应有利于探测并使噪扰报警和误报警减到最少。传感器位置选择应避免人为利用邻近的构筑物或物体逃避探测。

9.4.2 探测概率

传感器的选择和布置应保证室内入侵探测系统的探测概率在95%的置信水平下不低于90%。传感器应能探测到体重大于35 kg的入侵者以0.15 m/s~5 m/s之间的速度穿越探测场或屏障的行为。

9.4.3 报警条件

当室内入侵探测器探测到入侵行为时,应发出一个报警信号。

9.5 防篡改保护

传感器和相关的设备的箱体应设置防篡改开关或其他触发机械装置。当产生特定的触发条件时,防篡改装置应发出报警信号。应依照第12章来监管这些装置。

10 数据采集、处理和显示系统

10.1 设计原则

安保系统应能够从远程设备准确地采集数据,及时地分析数据,简明而又全面地显示必需的信息,同时保存报警、处理、命令和系统事件的历史日志。安保系统还应在发生报警时能够在保卫控制中心发出声光报警信号。

数据采集、处理和显示功能的设计应考虑适应性和保护措施。系统设计应考虑将来的扩容能力。安保系统还应考虑人因工程要求以便于操作。

10.2 数据采集

安保系统设计对数据采集的最基本要求是快速、可靠、准确地从远程设备将信息传送至中央存储单元,并进行处理。

系统设计宜考虑以下因素:

- a) 远程探测器的位置。数据传输类型和方式的选择需要结合考虑远程探测器的分布位置以及数据传输的距离和地形;
- b) 传输速度。远程设备状态变化传送到安保计算机主机的报警响应时间不大于2 s。同一通信链路上传输的所有设备在同一时间发出报警时的报警响应时间不大于2 s;
- c) 可靠性。数据采集采用的技术应确保远程传感器的探测报警信号能够及时有效传送。一个信号传输路径或元件失效(例如短路或开路)不应引起一个以上的探测点或信号传输点的通信失效。宜采用双重通信电路来传输一个以上报警点发出的报警信号;
- d) 处理能力。当核电厂发生突发事件、应急撤离、恶劣的天气或子系统组件故障等极端情况时,系统硬件和软件应具备处理大数据流量的能力。

10.3 信号处理

10.3.1 格式和兼容性

从远程设备接收到的信息应能转换成安保系统的各子系统、保卫控制中心的值班人员可使用的格式。转换的速度和可靠性应符合整个系统的性能要求。设计人员应考虑到10.3.2~10.3.8中所述的信号处理的因素。

10.3.2 速度

内部处理时间、数据转换速率和显示更新时间应保证从报警信号发生到显示的时间不大于1 s。

10.3.3 可靠性/可维护性

信号处理设备应提供自检程序以识别误操作。应提供冗余的处理器，以保证发生单一故障的同时，其中一台系统处理器处于维护期间时系统能可靠运行。

10.3.4 优先权

存在三种报警状态：

- a) 入侵；
- b) 故障；
- c) 篡改。

处理系统应将入侵报警信号状态设置为最高优先权。

10.3.5 实体防护措施

安保计算机系统应采取访问限制，包括硬件和软件两个方面。安保计算机系统应位于一个出入口控制的区域。没有设置在出入口控制区域的终端应按照安保计划相一致的要求限制其功能。所有的终端要求至少有密码开机程序。对于包括系统管理员操作的特定敏感的功能，应考虑增加额外的保护功能。系统应按操作人员登陆姓名记录操作日志。安保系统不应允许这些记录文件被编辑。

10.3.6 单点薄弱性

安保系统的主机服务器布置宜考虑避免因单个机房火灾、及水淹或丧失其他室内安置条件而导致整个安保系统瘫痪。宜独立设置冗余服务器电源设备、网络布线，及传输设备和器件的通信路径，以进一步避免因单一事件或者灾难而引起的系统操作全部失效。

10.3.7 扩展

安保计算机系统应具备可扩展能力。

10.3.8 报表生成

应提供自动的操作日志。存储数据的调用功能应与灵活调用各种信息。系统还应具备在线设计和生成定制日志报表的功能。

10.4 数据显示

10.4.1 数据显示的总体要求

数据显示应确定所需的信息及其显示的形式和格式。宜考虑保卫控制中心的值班人员整体工作负荷、理解能力和工作环境等因素。

10.4.2 格式和内容

安保系统设计应参考10.4.3~10.4.8中所述的数据显示的因素。

10.4.3 本地/远程设备的布置

应确定数据显示的形式和方法。应考虑人因的性能来提高数据显示画面的可操作性和可视性。

10.4.4 显示时间

内部处理时间、数据传输的速度和数据显示更新的时间应与从报警信号发生到显示的时间和远程显示设备的位置、整个系统成功地复核和显示报警信号的能力相一致，同时应满足10.3.2中的要求。

10.4.5 可靠性

数据显示的程序应采用技术手段，确保每当传感器传输指定的信号到显示设备时都能触发显示。当多路报警快速连续地从同一个地点或区域发出且没有其他报警关联时，它们宜作为一个组而不是多个单一报警的形式来触发显示。

10.4.6 安全性

应采取措施限制访问数据显示设备(硬件和软件)的控制部分。显示系统应采取措施防止通过显示系统设备对安保系统进行未经授权的访问。

10.4.7 可扩展性

数据显示设备应具备可扩展能力。

10.4.8 人因

显示系统在开发时应充分考虑人机交互界面，信息应易被值班人员理解。数据显示系统中对于报警输入信号至少应包括下列数据：

- a) 设备状态；
- b) 报警位置；
- c) 报警出现时间；
- d) 确认/未确认；
- e) 清除时间。

10.5 报警报告

10.5.1 报警报告的总体要求

报警事件发生在分散的各点或区域，由周界或室内入侵探测设备、门磁报警、读卡器读取故障，或其他安保探测设备触发。该报警报告应包含以下实时数据显示信息：

- a) 地点或区域标识；
- b) 控制点或区域的位置信息；
- c) 传感器触发的明显原因(例如,入侵)；
- d) 报警发生的日期和时间(精确到秒)。

应能提供未被清除的报警清单和历史报警记录。

10.5.2 设备故障报警

设备故障报警可使用10.5.1中描述的相同格式。特殊的有关计算机系统软硬件状态的重要报警，应使用与实物保护报警在同一界面显示。

10.5.3 值班人员的确认

安保系统应向值班人员提供一种确认事件的手段。系统应具备区分未被确认事件和已确认事件的能力。上述的区别应采用明显的指示方式来实现。

每个已确认的报警应被记录为永久的记录。永久的记录应包含已确认报警的时间和日期、地点或区域的确认、以及执行此操作的值班人员的身份信息。

10.5.4 报警注释

发生的每个警报应要求值班人员注释采取的具体行动。注释应有足够的文本以充分描述采取的行动。当多路报警快速连续地从一个单独的地点或区域发生且没有其他的报警插入时，它们宜被作为一个组来注释。

通知文本应被记录为永久档案，并应包含注释的时间和日期、地点或区域识别码以及执行这一操作的人员的身份识别信息。

10.5.5 事件清除与复位

报警系统应设计为只有当报警已被注释并复位后，保卫控制中心的值班人员才能将其从报警清单中清除。清除事件的行为应被记录为永久档案，并应包含清除的时间、地点或区域的标识、以及执行这一操作的人员的身份信息。

10.5.6 系统状态

报警点或区域的系统状态应实时显示。系统状态应包括各种报警情况包括报警、通行和离线等。

10.5.7 记录保存

生成报警报告的所有数据应作为永久的记录保存，并应以便于日后检索和调用的格式储存在备份的或大容量的存储设备中。

这些记录应依照核电厂的安保程序保存。

10.6 出入口控制系统的集成

10.6.1 内容

出入口控制系统与数据采集、处理和显示系统集成，可以便于人员通行的验证和文件的记录要求。

10.6.2 实体防护

传输到实物保护计算机系统的通行请求应包括用户的身份信息和授权进出的场所。首先应验证用于输入通行请求的出入口控制识别设备的有效性，然后应对照已存储的个人身份信息来验证识别数据。应验证通行请求的有效性以确定申请人是否在那个时间具有访问授权。以上任何一方面的否定或者不正确的回应都应发出一个警报。警报信息应包含未经授权的请求的日期、时间和地点，以及申请人的身份证明。应提供一种手段来记录所有已经授权和未经授权的通行请求。每发生一个访问请求都应记录在案。

存储设备应能生成一份含存储数据的周期性（通常是每天）日志。访问记录至少应包括访问的日期、时间、申请人的姓名和证件号码，以及请求通行的场所。未经授权的通行请求记录应包括最初的警告信息和采取的行动。

10.6.3 格式

出入口控制文件的生成格式应允许迅速且准确地输入数据。计算机数据库系统应采取措施避免因系统故障引起数据丢失。

10.6.4 与保卫控制中心计算机系统的集成

出入口控制系统应与保卫控制中心计算机系统集成，以灵活监测系统运行数据，例如实时分区人员统计、逻辑区域划分、来访者访问日志等。

10.6.5 与数据采集、处理、显示系统的接口

出入口控制系统的设计应考虑在执行核电厂应急预案程序时，仍具有数据采集、处理和显示功能。并在应急预案程序启动期间及之后，把指定的出入口控制点设为通行模式并按照应急预案程序提供人员清点的统计数据。统计报告至少应提供一份所有已清点人员的清单，及一份未清点到的人员及他们最后所处位置的清单。

11 安保通信系统

11.1 设计原则

保卫控制中心与保卫主管部门之间，与主控室之间应拥有两种以上双向通信手段，并且与保卫力量成员之间保持双向通信。此外，保卫力量所有成员间均应能够进行不间断的双向话音通信。

11.2 电话

电话通信系统用于保卫力量与核电厂运行人员之间的通信。宜设置一部与核电厂总机相独立的电话系统。

11.3 无线通信

应建立一个无线通信系统来实现实物保护响应力量的通信。

11.4 通信覆盖范围

现场安保通信系统的覆盖范围应做到覆盖保卫力量行动可能到达的场所，并实现不间断通信。

11.5 通信保护

集中式安保通信设备应设置在出入通行受控的区域，或应使用锁和防篡改报警设备进行保护。

11.6 天线防护

固定式安全无线电天线应设置在保卫区域内，否则应尽可能加以防护。

11.7 信息防护

安保通信系统的设计和运行应能限制外部人员通过监控网络获得信息（如采用加密措施）。

11.8 无线干扰的防护

安保通信系统的设计应具有防止核电厂运行设备的无线电频率干扰的能力。

11.9 通信丢失

当检测到通信性能下降或其中的一条通信中断时，应提供一种替代的通信手段，并立即启动修复工作。

12 线路监视

12.1 设计原则

线路监视是一种用于探测传感器与报警场所之间通信线路中的安保报警数据的被蓄意修改或故障的技术手段。

线路监视应用于所有的传感器数据通信线路，包括所有线路介质（例如，金属导线、光纤、大气传输）和所有线路类型（例如，专用线/星型结构、复用线/环形结构）。

12.2 连续探测

线路监视应连续地监视通信线路，包括记录相连接的传感器处于存取方式的时间。

12.3 及时探测

报警数据的改变应在不大于1 s的时间内被探测到并在保卫控制中心显示。

12.4 纵深防御

从传感器至报警器的每段数据通信路线都应有同等的保护。

12.5 均衡保护

每条安保报警的通信路线应有同等的保护。

13 胁迫报警

13.1 设计原则

胁迫报警设置在保卫控制中心、相关安报警卫室，及保护区域外的制卡中心等安保重要区域。另外，胁迫报警应考虑厂址内其它为满足安保计划需要的重要位置。这些附加的位置包括但不限于以下所列：

- a) 控制区主出入口；
- b) 主控制室；
- c) 保护区主出入口；
- d) 其他重要位置。

这种信号的发出可以使设施保卫人员察觉到敌对行为，例如某个威胁安全的武装分子或某个被胁迫的职员或其它紧急情况。但胁迫报警不应在胁迫威胁发生的现场显示。

13.2 胁迫报警设备

适用于各种工作位置的不同类型的胁迫报警装置，包括报警按钮、脚踏式报警按钮等信号发送装置。

13.2.1 报警按钮

手动式按钮报警器可以是保持式手动按钮或是有特殊颜色的墙装的需明显动作去操作的应急站。也可使用隐藏式按钮。

13.2.2 脚踏式报警按钮

脚踏式报警不需要太明显的动作去操作。如果使用者坐在桌子旁边，同时警报器嵌在桌子下的地板上，发出报警可秘密地操作。

13.2.3 出入口控制系统的胁迫报警功能

出入口控制系统具有可输入特殊规则的个人识别密码来发出已被胁迫的功能，胁迫码通过出入口控制系统自动识别发出的报警信息，此时报警发出人员的通行授权仍然有效，使报警能够秘密地发出。

13.3 胁迫报警的信号显示要求

任何胁迫警报装置应在保卫控制中心产生一个有别于其他报警的声光显示信号。

14 安保供电系统

14.1 设计原则

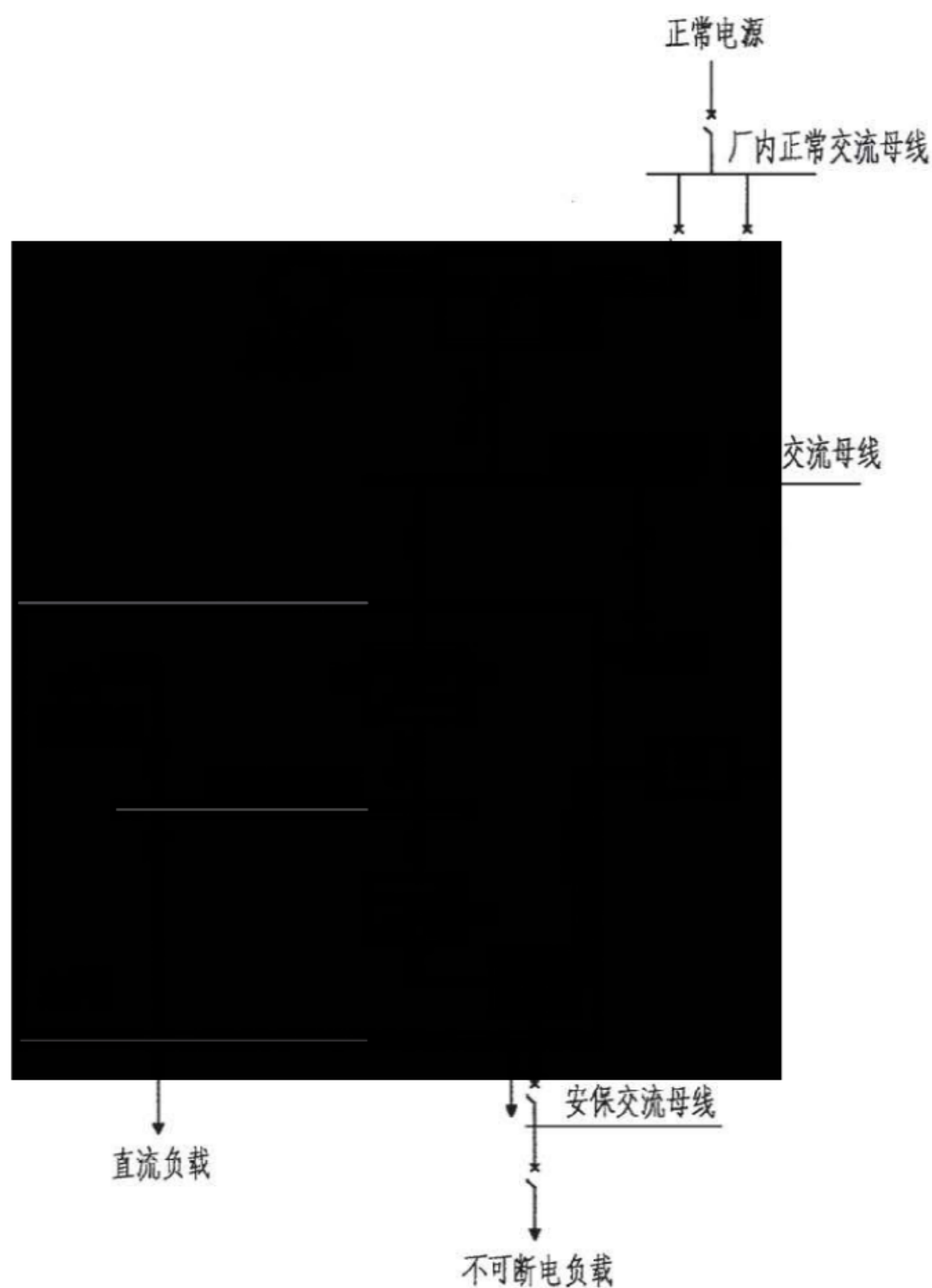
安保供电系统的设计及其设备安装应能保障安保系统的正常运行。

安保供电系统的设计原则是确保能对安保系统设备进行连续可靠供电。

安保系统的入侵报警系统、出入口控制系统、视频监控系统、集成化安保管理系统等均应由不间断电源系统供电，但是对于已具有备用电池的系统，或在安保功能不受影响的前提下允许其瞬间的短期失电的系统设备，如安保照明、安保通信系统等，可考虑设置应急电源。

不间断电源系统的自动开关和切换不应影响连续监测的数据完整性。不间断电源应能持续供电一小时而无需更换电池或给其再充电。当失去正常电源时，应急电源应至少支持所有系统设备连续工作24h。

一个典型的安保供电系统由发电装置、自动转换设备、检修旁路开关、正常交流供电回路组成（见图4）。发电机装置可以是专用的发电机组或是另一种能够满足同等要求的厂内电源。当正常电源失电时，由发电机装置向那些允许其瞬间短期失电的设备供电。



注1：此图为供电系统的简单图示，其他中间环节均未列出。特定的元器件类型不在此图中表示。

注2：AC — 交流电源

ATS — 自动转换开关

BC — 蓄电池充电器

DC — 直流电源

MBS — 检修旁路开关

RT — 调压变压器

SI — 逆变器

STS — 静态转换开关

UPS — 不间断电源系统

——> — 供电系统电力流向

图4 典型供电系统单线图

14.2 应急电源系统

14.2.1 设置位置

所有的应急电源设备应设置在保护区。报警显示设备和对讲主机设备的备用电源设置在有出入口控制的要害区。设备应能在其环境中正常运行。当有人破坏或非法侵入装有供电设施的区域，将会发出报警显示。

应急发电机组的燃料供应也应设置在保护区内，燃料的输入管道口也应采取保护措施。

14.2.2 不间断电源供电（UPS）系统

UPS系统应能向所有具有连续存储、监视功能的安保设备供电。这些设备包括系统计算机、系统显示器、打印机、报警装置、多路复用器、视频监控设备、周界入侵探测设备、内部入侵探测设备、门禁设备（诸如刷卡器、出门按钮等）、旋转栅门、通信设备等。

一个典型的UPS系统主要由一路正常电源、一套静态逆变器、一套静态转换开关、一套检修旁路开关、一套蓄电池充电器、一套蓄电池组及一路备用交流电源组成。

14.2.3 厂用供电母线

UPS系统交流备用供电和正常供电应来自独立的厂用母线段。厂用母线段应能提供内部或外部电源。调压变压器为UPS提供交流备用电源，总谐波畸变率不应大于5%。

14.2.4 电池组

当应急不间断或安保电源（见图4）无法为应急照明设备供电时，由电池组为其供电。电池组用来在应急电源启动前的断电期间内为安保岗位和安保区域的照明供电。电池组的运行时间由供电中断时间来决定。

14.2.5 自动转换开关

UPS系统的自动转换不应对安保供电系统造成影响。自动转换宜在四分之一周内完成。

在充电器故障时，UPS系统应能通过蓄电池组维持系统正常运行。在正常电源失电时，另一路交流电源应能维持系统正常运行。电池的运行时间或另一路交流电源提供的时间由供电中断时间来决定。

利用检修旁路开关应能安全地对UPS进行维护和检测。

14.2.6 显示

应急电源或UPS系统的异常运行状态应在保卫控制中心显示并发出报警。这些报警包括：正常电源失电、备用交流电源失电、不同步、从备用交流电源得电、逆变器故障等。

14.2.7 容量

安保供电系统应能向所有安保系统设备供电。安保供电系统应在负荷满载情况下，也能使最大的负载或电机带电运行，并且不会由于电压降低造成其他安保设备供电丧失。供电容量应预留出25%的计算负荷裕量。

15 维护及测试

15.1 设计原则

应在安保系统寿期内建立并维护维修和试验程序。在维修和试验程序中应至少标明：

- a) 承包商地址和验收测试的地点；
- b) 设备识别方法；
- c) 定期测试、校准和其它维修的程序；
- d) 测试和预防性维护的时间间隔；
- e) 记录档案和档案管理及配件；
- f) 技术上的资料的管理；
- g) 培训。

集成安保系统设计应具备性能试验的能力，并宜具备日常维修能力，使系统功能失效时间减至最短。测试和维护安保设施的程序应满足设施安保程序要求。

15.2 验收测试

应在出厂前建立完成部件、系统组件和系统验收测试的大纲。至少应在系统投入运行前在核电厂现场对已安装的系统进行验收测试。

15.3 设备标识

应编制安保系统中全部设备的清单，以便适当地识别每个物项。每个物项或部件都应分配一个识别码，并将识别码贴在或刻在对应的物项上。识别码记录应包括类型和序列号。

15.4 程序

根据设备类型编写的程序应适合每个维修功能。至少在进行测试和校准时应编制和使用备有证明文件的程序。程序应至少包括但不仅限于下面的基本信息：

- a) 被试验或校准的物项的标识；
- b) 包含最后校准日期的试验设备的描述；
- c) 试验或校准以及适当的公差描述；
- d) 试验或校准的顺序；
- e) 专用的说明书。

用日历时间或运行时间表示试验或校准的频度。

15.5 试验周期

试验周期和定期维修的程序应依据设备固有的可靠性记录、试验所需的停止工作的时间、类似设备的历史记录以及调整的需求来确定。

15.6 记录

在设备、系统和子系统的寿期内，应保存所有初始试验的记录，除非另外证明不需要记录。保卫设备的校准、预防性或纠正性维修、或设备更换的记录应保存三年。记录应能通过编号、完成的工作的性质、所用规程和试验设备（如需要）、试验日期和完成试验工作的人员来识别设备。

15.7 备件

为了使系统性能保持在可接受的水平，应当建立备件采购和存储体系。设备供应商的建议和设备故障的经验可以用来建立适度的、保有的备件库存量。

15.8 技术资料

技术资料，例如维修手册、系统图和接线图，应在设备安装前就获得，并应作为设施记录管理程序的一部分在设备或系统的寿期内维护。当系统或设备的个别物项发生改变时，技术资料和图纸就应按照设施管理程序来进行更新。

15.9 培训和认证

在安保系统安装之前，应启动维修人员的培训和认证程序。安保系统的维护培训的记录宜在维修人员任职期间一直维护并保存。

参考文献

- [1] GB 50343—2004 建筑物电子信息防雷技术规范
-

中 华 人 民 共 和 国
能 源 行 业 标 准
核电厂实物保护系统设备准则
NB/T 20147—2012

*

原子能出版社出版
核工业标准化研究所发行
北京海淀区骚子营 1 号院
邮政编码：100091
电话：010-62863505
总装备部军标出版发行部印刷车间印刷
版权专有 不得翻印

*

2013 年 3 月第 1 版 2013 年 3 月第 1 次印刷
印数 1—200