

中华人民共和国能源行业标准

NB/T 20027—2010

核电厂主控制室的报警功能与显示

Nuclear power plants-main control room-alarm functions and presentation

(IEC 62241:2004, IDT)

2010-05-01 发布

2010-10-01 实施

国家能源局 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 背景解释	5
4.1 报警系统存在的问题	6
4.2 功能设计要素	6
4.3 其他因素	6
5 基本功能要求	7
5.1 报警功能	7
5.2 报警信号	8
5.3 报警信号处理	8
5.4 报警显示处理	8
5.5 报警控制和管理	9
5.6 报警显示和显示—控制集成	9
5.7 人因	10
5.8 评价	10
6 报警设计定义	10
6.1 概述	10
6.2 关键报警	11
6.3 必要报警	11
7 报警信号处理	11
7.1 概述	11
7.2 报警信号确认	11
7.3 报警产生和精简处理	12
7.4 事件序列和延时处理	13
7.5 首出处理	13
8 报警显示处理	13
8.1 概述	13
8.2 组合报警	14
8.3 报警抑制	14
8.4 暗盘原则	15
9 报警控制和管理	15
9.1 概述	15

9.2 声音警告和消音.....	15
9.3 闪光和重闪.....	15
9.4 确认.....	16
9.5 回铃.....	16
9.6 复位.....	16
10 报警显示和显示—控制集成.....	18
10.1 概述.....	18
10.2 报警盘和报警光字牌.....	20
10.3 VDU 报警列表画面.....	20
10.4 音响报警.....	22
11 可靠性, 试验和可维修性.....	22
11.1 可靠性.....	22
11.2 试验.....	22
11.3 可维修性.....	23
12 报警记录.....	23
13 报警响应规程 (ARP).....	23
13.1 概述.....	23
13.2 内容.....	23
13.3 格式.....	24
附录 A (资料性附录) 报警系统问题.....	25
附录 B (资料性附录) 触发报警的信号源.....	26
附录 C (资料性附录) 报警处理逻辑和动态优先级举例.....	27
附录 D (资料性附录) 报警分组和分类概念举例.....	29
附录 E (资料性附录) 区别报警和状态信息所需的素材.....	30
附录 F (资料性附录) 报警光字牌排列样例.....	31
附录 G (资料性附录) 报警分类考虑要点举例.....	32

前 言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准使用翻译法等同采用IEC 62241:2004《核电厂 主控室 报警功能与显示》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB/T 13630-1992 核电厂控制室的设计（IEC 60964:1989, eqv）；
- GB/T 15474-1995 核电厂仪表和控制系统及其供电设备安全分级（IEC 61226:1993, NEQ）；
- EJ/T 759.2-2000 核电厂控制室控制器和屏幕显示的应用 第2部分：屏幕显示的应用（IEC 61772:1995, eqv）；
- EJ/T 1118-2000 核电厂控制室设计验证和确认（IEC 61771:1995, MOD）；
- EJ/T 1143-2002 核电厂控制室设计功能分析与分配（IEC 61839:2000, MOD）。

本标准做了下列编辑性修改：

- 删去 IEC 标准的前言和引言；
- 简化第1章“范围”的内容。

本标准由全国核仪器仪表标准化技术委员会（SAC/TC30）提出。

本标准由核工业标准化研究所归口。

本标准主要起草单位：中广核工程设计有限公司。

本标准主要起草人：徐晓梅、江国进、史凯、詹林钰、叶王平、昌海、于正龙、刘素娟。

核电厂主控制室的报警功能与显示

1 范围

本标准确立了核电厂主控制室报警系统功能设计的基本原则。

本标准适用于核电厂主控制室报警功能和报警显示的设计。

本标准不适用于核电厂火灾报警系统、安全报警系统等特定报警系统的设计。

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。

IEC 60964:1989 核电厂控制室设计 (Design for control rooms of nuclear power plants)

IEC 61226 核电厂 安全重要的仪表和控制系统 分级 (Nuclear power plants – Instrumentation and control systems important for safety – Classification)

IEC 61771 核电厂 主控室 设计验证和确认 (Nuclear power plants – Main control room – Verification and validation of design)

IEC 61772 核电厂 主控室 屏幕显示器 (VDU) 的应用 (Nuclear power plants – Main control room – Application of visual display units (VDU))

IEC 61839 核电厂 控制室设计 功能分析和分配 (Nuclear power plants – Design of control rooms – Functional analysis and Assignments)

3 术语和定义

下列术语和定义适用于本文件。

3.1

报警 alarm

用于诊断、预兆或导向的相关信息，警告操纵员关注过程变化或系统偏离。

注1：报警所提供的特定信息包括：存在的异常、异常原因和潜在后果、整个电厂的状态、针对异常所要求采取的纠正措施以及采取纠正措施后的反馈。

注2：偏离可分成下述两类：

- a) 非预期的偏离，即非预期的工艺偏离或设备故障；
- b) 预期的偏离，即在预期可控的非正常电厂条件下，工艺条件或设备状态的偏离是期望出现的正确响应。

3.2

报警确认 alarm acknowledgement

需要操纵员实施的动作，用于表示操纵员已识别所呈现的报警。

3.3

报警雪崩 alarm avalanche

大量报警在短时间内出现，出现速率超出操纵员处理能力的一种状况。

3.4

报警编码 alarm coding

用一定的视觉和听觉方法突出所关注对象，以进一步提高操纵员对该对象的关注。

3.5

报警控制 alarm control

报警显示的控制功能，用于支持操纵员及时、正确识别报警状态。

注：报警确认、消音、复位是三种典型的“报警控制”实例。

3.6

报警显示处理 alarm display processing

用于控制或改善报警显示的报警信号处理功能或机制，例如，组合报警、报警抑制。

注：报警显示处理的对象是报警信号处理逻辑所标识的报警(见3.15)。

3.7

报警盘 alarm fascia

由一组报警光字牌组成的报警显示方式。

3.8

报警精简或过滤 alarm reduction or filtering

为减少报警数量和提高操纵员的关注度而对报警信号处理的功能或机制。

注：过滤和精简是通用术语。

3.9

报警产生 alarm generation

报警信号处理的功能或机制，用于根据预定义报警信号和非报警开关量信号（如设备状态信号）的逻辑组合来生成报警。

注：见“报警信号处理逻辑”。

3.10

报警标志 alarm legend

标识一个报警的说明。

3.11

报警消息 alarm message

标识一个报警的短语，典型地用于VDU报警显示。

注：它可与补充信息关联，如报警触发时间、阈值及工艺变化趋势。它也可以用一段语音来表示一个报警，它可以与规程或其他补充信息关联。

3.12

报警优先级 alarm prioritization

对报警按重要性分级的报警信号处理功能或机制。

注：优先级可预先定义或根据电厂工况动态确定。

3.13

报警记录 alarm recording

使用永久记录如打印、长期磁介质或光介质保存，确保每个报警的标识、报警出现时间和报警消失时间以及报警信号可以用于离线研究和分析。

3.14

报警信号 alarm signal

输入到报警系统、经处理后可产生一个报警的开关量信号。这些信号也可能是电厂或仪表和控制(I&C)系统的原始信号。

3.15

报警信号处理 alarm signal processing

在识别报警并传递给报警显示处理单元显示给操纵员之前(见第7章和5.3),对报警信号进行处理的逻辑或机制。

注:报警信号处理用于报警信号确认、报警产生、报警精简或优先排序。

3.16

报警信号确认 alarm signal validation

报警信号处理功能或机制,用于确定报警信号是否正确表达了相应的工艺或系统状态。

3.17

报警消音 alarm silence

用于停止与报警相关的声音提示或警告的动作。

3.18

报警抑制 alarm suppression

阻止对当前运行无关的报警信息显示的一种功能。

注:被抑制报警的状态仍可以通过其他方式确定。

3.19

报警系统 alarm system

用于向操纵员警示出现异常(系统或工艺的偏离)的系统,并且该异常可能需要采取纠正措施。

注:报警系统通常是I&C系统的组成部分,尤其是计算机化I&C系统,但对于硬接线的I&C系统,也可以是一套独立的设备。

3.20

报警阈值 alarm threshold

过程值或系统状态,可作为一种参照,用于触发一个报警信号。

注:亦称报警限值或报警整定值。

3.21

报警光字牌 alarm tile

刻有标题并且当报警出现时能点亮的瓦片状报警显示单元。

3.22

警示 alerting

用视觉和听觉信号来进行警告的动作,用于提高操纵员的关注度。

3.23

暗盘 dark-board

作为报警显示设计的目标之一,使电厂在正常状态下无报警显示。

3.24

不一致指示器 discrepancy indicator

当指示器开关或控制设备开关的状态与其控制或显示的最终状态不同时,点亮指示器开关或控制设备开关上的灯。

3.25

动态报警编码 dynamic alarm coding

报警显示处理功能或机制,用于动态改变报警编码(例如:报警呈现的颜色)。

注:依照动态优先级通过不同颜色点亮报警光字牌是动态显示编码的实例。

3.26

首出报警 first-up alarm

一组相关报警中的第一个触发的报警。

注：通常用于表示引起反应堆保护系统或安全系统动作的第一个信号。

3.27

组合报警 grouped alarm

由几个报警进行逻辑组合后生成的报警。

注：通常使用逻辑“或”门来生成组合报警。有时亦称“共享报警”。

3.28

分组 grouping

根据物理或功能特性对报警进行组合。

注：按特定方式在某个地方布置一组报警的做法是根据物理特性分组的一个实例。

3.29

导航 navigation

VDU方式信息系统中用于支持操纵员定位所需信息和画面选择的导向功能。

3.30

干扰报警 nuisance alarm

在出现和消失两个状态之间重复循环、可导致分散注意力或造成烦恼的报警。

注：亦称“反复报警”。

3.31

重闪 reflash

当报警消失后重新出现、或者用于指示组合报警中有新报警触发，使报警标题闪光或通过VDU上图形闪光来再次呈现报警的动作。

3.32

复位 reset

报警控制功能，用于将已消失报警清除显示使报警系统返回到预定义状态。

3.33

回铃 ringback

报警呈现功能，用于表示报警条件已清除。

3.34

持续报警 standing alarm

已确认但仍呈现的报警。

3.35

提示语 telop

在VDU显示画面页脚或页眉显示的、通常带有数字内容的简短消息或符号，用于指导用户进入另一幅显示画面或通知用户相关信息，如重要报警的数量。

4 背景解释

4.1 报警系统存在的问题

报警系统的不完善设计有时引起人因问题，而这些人因问题可能对电厂可用性及安全是致命的。典型的人因问题包括：

- a) 忽视重要报警；
- b) 延迟探测重要报警；
- c) 负荷过多增加而影响其他运行活动的完成；
- d) 疏忽频繁触发的报警；
- e) 因误解报警之间的关系以及各报警的重要性而导致的困惑；
- f) 当操纵员知道机组已发生变化（相应）报警延迟出现将降低操纵员对报警系统的置信度。

上述人因问题的主要原因在于：

- a) 大量报警的瞬时触发，导致操纵员不能及时确认。这个问题也称“报警雪崩”。另外，大多数这类报警对运行不具备必要的意义而只是与其他更有意义的报警相关；
- b) 干扰报警和持续报警；
- c) 正常运行工况下触发的无意义报警；
- d) 在电厂换料大修期间出现、或由于维修或定期试验引起的大量报警；
- e) 运行习惯，为了对付人因困难，操纵员趋向于创建自己的运行习惯。比如，有些操纵员在瞬态发生后不立即确认报警。这种处理能减轻增加操纵员负荷的问题，但可能导致对重要报警的探测延误；
- f) 现有报警系统中报警信号处理和报警显示处理的设计局限。

更为重要的是，如果所有系统设计者考虑下述方面的内容，这些问题就可减少：

- a) 根据给定条件对每个报警运行价值的清楚定义；
- b) 报警之间的动态关系；
- c) 报警信号处理逻辑和报警显示处理方法的合理实施。

本标准的主要目的在于，通过明确规定功能要求及本标准给出实施建议来减少人因问题。

报警系统问题的补充信息参见附录A。

4.2 功能设计要素

图1是本标准范围内报警系统功能设计相关组成要素的概念结构图。实际的硬件、软件配置可能因I&C系统配置、设计者选择或其他因素而有所不同。

本标准对于报警系统设计主要考虑如下五个要素：

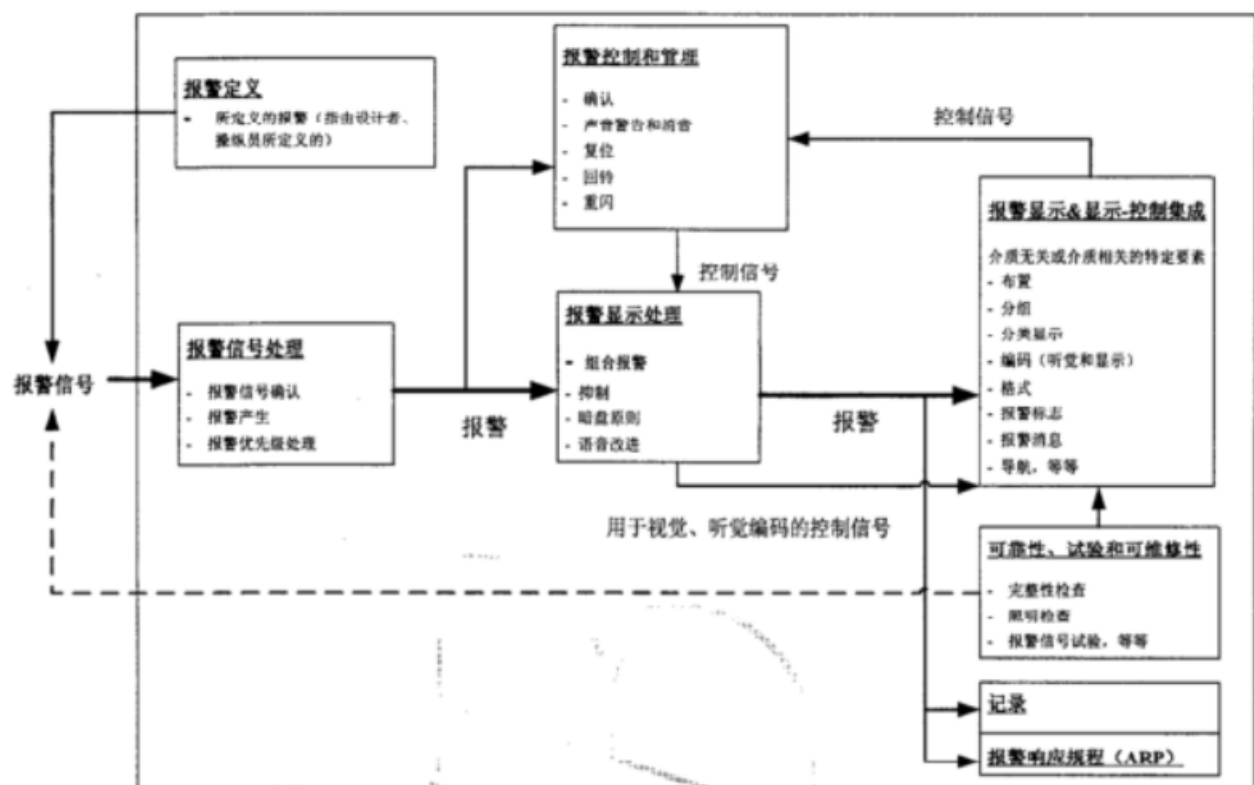
- a) 报警定义；
- b) 报警信号处理；
- c) 报警显示处理；
- d) 报警控制和管理；
- e) 报警显示和显示—控制集成。

4.3 其他因素

本标准还包括如下报警系统重要功能设计要素：

- a) 可靠性；
- b) 试验；
- c) 可维修性；
- d) 记录；
- e) 报警响应规程（ARP）。

在送往报警显示处理单元之前，在报警信号处理单元中，应确定报警信号的特定条件以定义一个真实的报警。详细的要求见第7章。



注：此功能结构是组成本标准的基础，可以由不同的硬件结构实现。

图1 报警功能设计要素

5 基本功能要求

5.1 报警功能

报警系统应探测电厂非预期变化并经报警信号处理后产生报警，用于报警显示处理和报警显示。

报警应提供操纵员足够的警示信息，以判断存在安全风险或事故、电厂扰动、电厂及设备故障、以及其他事件，报警功能至少提供如下基本信息特征：

- a) 告知操纵员异常的存在以便操纵员能够开始采取纠正措施；
- b) 通知操纵员电厂出现导致电厂系统状态或状况发生变化的故障、扰动和非预期事件；
- c) 引导操纵员获取进一步诊断和理解所发生事件需要的信息，有助于计划和实施纠正措施；
- d) 帮助操纵员确认电厂总体状态。

报警显示系统总体设计时宜考虑下述补充功能：

- a) 向操纵员提供事件原因和后果相关的信息；
- b) 引导操纵员到达整个控制室信息系统的入口点；
- c) 向操纵员提供运行规程的适当查询手段。

另外，应考虑减少由于报警系统本身造成的分散操纵员注意力、干扰报警和增加操纵员负荷等情况。应明确报警系统的性能要求。

5.2 报警信号

5.2.1 概述

报警信号通常以双态输入或一组模拟量输入的阈值比较结果方式提供，用于满足5.1的报警信号产生和显示处理功能要求。报警信号定义可能由电厂设计者负责，但是如果假定这些信号总是代表报警，或这些信号出现时报警总是显示，那么对重要报警的忽略或报警雪崩等相关人因问题可能会发生。因此，如何对这些信号进行报警定义以及如何进一步的显示方式的处理是需要考虑的。

5.2.2 报警信号的基本要求

提供电厂的报警和支持信息应足够充分，并包含适当的操作信息并满足技术上的一致性。

报警定义宜遵从IEC 61839的功能分析结果。报警系统应提供保证安全和有效运行所需的报警。

报警信号宜包括电厂状态和控制开关状态指示信号，用于包括维修、换料大修、停堆和其他工况下进行的适当的报警处理逻辑。

详细要求见第6章。

5.3 报警信号处理

5.3.1 概述

报警信号处理用于从输入报警信号中甄别出有效的报警信息。只有真正需要操纵员注意或采取行动的工况才生成报警。因此，报警信号处理需要识别这些工况，并减少操纵员必需的动作。需要确认报警信号的有效性以避免使用无效信号。报警信号处理需考虑报警信号生成或消除时的电厂状态和其他报警条件。

5.3.2 报警信号处理基本要求

产生真实报警工况的特征可包括如下一项或者多项：

- a) 对电厂运行的功能性扰动，需要操纵员立刻或短时间内执行控制室操作；
- b) 用于缓解和控制电厂扰动风险和超限运行所执行的自动动作；
- c) 设备故障工况，要求或标明一项恢复设备功能或运行的维修或就地操作正在进行。

对于报警信号指示的其他报警工况，将它们纳入到主控室的真实报警之前，宜仔细检查。

宜建立用于识别更重要报警信号的系统化技术体系，这可结合如下所有或部分功能予以完成：

- a) 报警信号有效性确认；
- b) 报警产生和精简；
- c) 报警优先级。

在报警显示处理之前，报警信号处理应根据报警信号确定指示真实报警的特定工况。

这些要求的详细描述参见第7章。

5.4 报警显示处理

5.4.1 概述

报警显示处理使用清楚显示报警、报警分组、抑制“干扰报警”、允许选择抑制“持续报警”、运用颜色或其他方式进行显示编码等手段，优化操纵员对报警的察觉和认知。报警盘和报警光字牌可以从物理空间上分组布置，目的在于减少每种运行工况下报警数量以突出安全相关重要报警和提高运行效率。

5.4.2 报警显示处理基本要求

报警显示处理应能够有助于操纵员对报警重要性的识别。宜具备如下功能：

- a) 当探测到报警时，显示报警标志或消息，同时有闪光或相关字符闪光及声音警报；
- b) 报警雪崩的处理和显示；
- c) 持续报警的处理；
- d) 干扰报警的处理；
- e) 根据电厂分区或其他特性的报警分组；
- f) 带有报警出现和报警消失时间的显示和记录。

实现上述功能的详细方法见第8章。

5.5 报警控制和管理

5.5.1 概述

报警控制和管理功能包括：报警确认、音响警告、在报警盘或VDU上复位报警、在VDU上选择特定显示功能。控制相关的报警显示方式，如报警重闪（报警再次出现时闪光）或报警回铃（报警消失时再次显示），也属于控制范畴。

5.5.2 报警控制和管理基本要求

对报警显示的功能设计应确保操纵员能注意到每个报警。下述报警控制功能宜具备：

- a) 报警出现时，消除报警音响；
- b) 报警出现时，确认每个报警；
- c) 报警消失时，回铃指示；
- d) 复位以清除已消失的报警；
- e) 报警再次出现时的重闪。

实现上述功能的详细方法见第9章。

5.6 报警显示和显示—控制集成

5.6.1 概述

为达到电厂安全及运行目标，作为信息系统的一部分、以及作为决策和控制的出发点，操纵员需要一套完整的报警显示方法。报警显示的方式包括使用常规报警盘及报警光字牌、VDU、大屏幕和挂壁式显示盘。在选取显示方式、显示布局、报警控制操作、报警标题或消息、VDU方式下的详细的显示方法时，需要重点关注清晰性和可操作性。

5.6.2 报警显示和显示—控制集成的基本要求

报警信息的物理显示形式及其布局和分组，应结合5.3至5.5所列的功能和技术要求精心设计，以实现相关功能和满足5.1的要求。

需强调的是，任何报警显示方法的使用宜确保在报警高负荷状况下系统基本功能的维持，即对于需要操纵员立即采取行动的、或者威胁到电厂重要安全功能的报警（高优先级报警），应以一种能支持操纵员在任何报警负荷条件进行快速识别和理解的方式来呈现。因此，基本要求如下：

- a) 对于高优先级报警宜提供特定显示位置；
 - b) 在指定的显示介质上显示的报警，应根据功能、电厂系统或其他合乎逻辑的方式来进行分组。
- 此外，设计应体现下列显示特性：
- a) 编码；
 - b) 呈现特征（如：显示格式）；

- c) 标题及信息清晰一致;
 - d) 导航方式。
- 实现上述功能的详细方法见第10章。

5.7 人因

报警系统的设计应符合其他人机接口相关的标准和惯例,也应与相关运行规程相符。因此,设计者不应孤立地设计报警,而是将报警作为整个信息系统的组成部分,从最终满足人因和有益于运行方面来进行设计。

所要关注的特定要素包括:

- a) 信息内容及覆盖面;
- b) 术语和缩略语的使用,如:在VDU显示方式和报警光字牌方式下都应保持信息的清晰性和一致性;
- c) 编码和其他人因标准和惯例,如:要保持VDU显示方式和报警光字牌方式编码的一致性。

应确定报警系统设计人因准则和导则,并系统化加以应用。宜参照适当的人因标准和导则。

主控制室设计组应关注报警系统的设计。可任命一位报警系统设计协调员。应确保全面而充分地考虑人因和安全问题。

设计中,宜选择增加操纵员对报警的关注度并要求确认动作的主要方法。通常应是报警信息的列表,以确保报警被明确标识和记录。报警信息列表、工艺流程图或模拟图以及报警状态变化的指示(报警激活或被消除状态间的变化)应使用相同的符号和惯例。

5.8 评价

应遵照IEC 61771进行性能评价以确保有效达到所期望的系统性能。特别是,应选择一种报警雪崩工况,在此工况下系统应能够在许可的延迟时间内将所有报警呈现给操纵员。

6 报警设计定义

6.1 概述

应根据IEC 61266对报警功能进行分类。报警分类时要考虑的要点参见附录G,这同时也决定了用于实现报警功能的设备分级。

报警范围、信息源及其统一的设计原则宜在电厂设计初期加以明确。为了审查确定修正要求,报警范围宜在最初设计中确定。审查宜确保与最初设计原则一致,并包括在清晰定义的修正原则下的新的信息源。

报警定义所需信息的原则宜保证提供足够的信号以监测下述功能为基础:

- a) 重要安全功能的状态;
- b) 可能的人身伤害;
- c) 安全功能设备的损坏或故障;
- d) 影响运行目标的电厂工况。

注:对于重要安全功能,参见IEC 60964的A3.1.1,其列举内容如下:反应性、冷却剂装量、堆芯热量排出、热阱、反应堆冷却剂系统完整性、安全壳系统完整性,或参见IAEA导则。

6.2 关键报警

报警功能应由与其安全分级相符的仪控设备实现。对于一般报警功能，如果所使用的设备不满足所需要的最高安全分级，额外增加一更高安全级别的报警设备可能是必要的，用于支持下述功能：

- a) 当电厂计算机系统或集成报警系统不可用时保持电厂安全稳定运行；
- b) 当电厂计算机系统或集成报警系统不可用的情况下出现一个关键报警时执行电厂安全停堆；
- c) 验证和确认机组达到安全停堆。

当电厂计算机系统或其他集成报警系统不能提供足够的可靠性用于确保达到安全运行和停堆时，应采用上述原则。

6.3 必要报警

报警的必要性及其重要度宜从运行角度而不是只站在单个独立系统设计的角度来定义以保证其合理性。提供报警信号（经报警信号处理逻辑产生报警显示）的报警工况包括：

- a) 与电厂连续运行相关的参数测量或者电厂安全重要的参数测量以及异常工况的阈值核查；
- b) 多阈值检查的参数测量，用于探测偏离正常工况，或者探测异常工况的进一步恶化，如用于停堆和安注；
- c) 电气或机械设备的异常状态，如阀门、泵和其他设备；
- d) 自动动作或序列的失效，或不完整动作，如：自动功能的自监督、自动顺控或设备的运行监视（非预期失效产生报警）；
- e) 电厂系统实际状态与需求状态不一致（如：闭环控制未能产生期望结果、控制设备合闸但断路器没有关闭）；
- f) 基于计算机或其他仪表、报警处理和显示系统和控制和保护系统的异常或故障以及自诊断功能结果；
- g) 特别地，计算机系统局部供电丧失、计算机系统冗余丧失、计算机化系统或其他提供报警的主要系统丧失。

那些不需要操纵员考虑或响应的信号不宜用于主控制室报警。

报警系统应具有备用容量和设施用于变更。

典型的报警信号源参见附录B。

7 报警信号处理

7.1 概述

报警信号处理宜确保在所有电厂工况下只选取有效和相关的报警进行实时显示，限制出现不相关的报警。

报警信号处理宜确保已经出现的报警得到正确的探测和记录。

7.2 报警信号确认

传感器和输入信号宜通过在线确认，以确保由于传感器或报警输入设备失效导致的虚假信息不会产生报警。

有关模拟量信号的在线有效性认可，其合适方法可能包括检查电信号及测量值是否在可接受的范围。触点信号和双态信号在线有效性认可方法可能包括探测线路故障的设备，如错误的接地隔离和触点去抖动的过滤方法。

依赖于任何有缺陷的输入或输入设备失效产生的报警和信息，在显示的时候宜通过标识或其他方法指示为有缺陷。

7.3 报警产生和精简处理

7.3.1 报警产生和精简处理的要求

报警信号处理逻辑应用于产生报警，并根据功能包括的运行重要性来限制或减少报警数目：

- 确定运行、维修或停堆模式，并以此分配一个报警信号给信息或报警显示方式；
- 报警信号及其产生的报警的优先级定义，可以通过先前固定的优先级、动态确定的优先级，或与其他报警比较的相对优先级来确定；
- 减少报警数量，只保留对当前运行重要的报警信息；
- 在电厂保护动作或者其他情况下出现报警雪崩时，应采用减少报警数量处理方法。

当设计要求产生报警时，应符合以下条件：

- 报警信号和其他用于产生新报警的信号应予以鉴别；
- 生成报警的方法或逻辑的定义应形成文件，并被设计者和用户所知道；
- 在异常工况下，应通过报警处理技术来减少显示给操纵员的报警消息数量，以支持操纵员能够在必需的时间内探测、理解和处理所有对于电厂工况重要的报警；
- 报警抑制、报警减少和优先级处理宜得到应用。

报警信号处理可以用来对报警信号列表或者分组，或者减少报警的数量。可以使用带延时的与、或、非逻辑，或其他定义的逻辑以生成一个报警以及组合报警或标识报警的优先级。

报警处理逻辑可以根据与电厂运行工况的关联或其他报警信号的条件，来判定将一个报警信号划分为或不划分为显示处理的一个报警，所采用的方法参见附录C。

7.3.2 报警优先级

对报警进行优先级划分的目的是给操纵员提供确定报警重要性的指导。为了维持对电厂变化的关注，优先级不宜成为报警抑制的依据，因为报警抑制会影响操纵员了解所需运行相关的电厂变化。

优先级划分可以通过将每个报警分配一个优先级来实现。为了避免混淆，优先级的分级应尽可能少（例如：3—5级）。

报警优先级的确定可以是报警信号处理的一部分。决定报警优先级最重要的是工况的严重性和后果。报警的优先级可以设计成固定的或者通过动态方式决定。

可以采用以下分配优先级的方法：

- 固定优先级基于报警的静态重要程度。按照每一个报警的重要程度对报警进行分级，报警重要程度取决于对电厂的影响、可能的放射性物质释放、以及要求操纵员处理的紧急程度；
- 动态优先级基于报警的动态重要程度。报警信号处理逻辑运用所产生报警信息和当前电厂运行（例如：正常运行期间，异常工况，事故工况）之间的关系，那时的重要报警和次要报警根据优先级进行区分。

固定优先级是简单的，但也许不能体现所有电厂状态下的最优的优先级分配。动态优先级可以达到更精确的优先级分配。但存在一定风险，即尽管有非常高的工程效果，但有可能无法得到令人满意的一致性。具体如下：

a) 固定优先级

当使用固定优先级时，报警可能在设计阶段时定义为某个优先级，例如：高，中，低，这一优先级将用于任何时候的显示。

有些报警的优先级可以通过调整需求得到确定，或者相反，始终处于那些定义的等级，报警产生逻辑应考虑这些需求。优先级可能有两个等级：

- 需要执行事故后操作规程或需要进入事故后运行模式的报警处于最高优先级；
- 指示安全系统的可用性降低的报警；

3) 其他报警。

b) 动态优先级

当采用动态优先级时,动态报警优先级方案宜能够通过与其他报警比较或考虑给定的电厂工况动态确定相关报警重要性高或低,并可随着时间推移而改变。相关基准如下:

- 1) 要求采取纠正行动的紧急程度;
- 2) 报警工况对电厂工况影响的严重程度。

严重程度可能在设计阶段进行定义,但是采取纠正行动的紧急程度通常取决于运行情况,也就是应由动态的方式决定。基于故障后果,重要性的动态优先级划分可分为三类:

- ◆ 报警组 1, 要求操纵员采取相应的行动的报警;
- ◆ 报警组 2, 要求操纵员确认电厂工况的报警;
- ◆ 报警组 3, 不要求操纵员必须采取相应的行动或确认的报警。

更多关于报警产生、动态和相关优先级分配、报警过滤和减少的方法的信息参见附录C、附录D和附录E。

7.4 事件序列和延时处理

报警系统宜有这样的能力,通过对报警信号进行时间滤波和时间延迟,从而滤去噪声信号,并消除不必要的瞬间报警。

报警延迟可用于报警产生和报警精简处理,以及监视事件序列。使用时间处理的例子包括:

- a) 在报警雪崩期间,对某些报警的显示或优先级将进行调整,直至电厂工况稳定为止;
- b) 在电厂某一物项(如泵)的启动或停止过程中,通过时间限制以鉴别设备运行故障;
- c) 自动顺控运行中使用时间限制,以确认事件正在采取正确的路径或提供故障的警告。

更多信息参见附录E。

7.5 首出处理

为了有助于事件诊断和根本原因分析,宜规定使用首出报警的方法来鉴别与电厂自动脱扣相关的始发事件。

8 报警显示处理

8.1 概述

当探测到报警时应将其显示出来,并且报警标志或报警信息应在合适的介质上显示(见10.1.2)。当报警开始显示时,应有一个关联的闪光标志或者闪光符直至被确认(见9.4);同时伴有一个声音警告(见9.2)直到消音。

当报警在标牌上消失时,该报警标识可能立即被清除或仍然点亮直到手动复位(见9.6),或有一个相关的回铃动作(见9.5)。设计应识别对每个报警指定该采取哪种行动,并且应有不同的符号来表示。

当一个报警从VDU上清除时,应提供一种方法,明确表示它的状态现在已被清除。可以使用替代的方法,但宜谨慎。

减少混淆风险的方法包括:

- a) 只有在报警消息显示和可见并直接由操纵员执行报警控制和管理动作后才可从清单中移除该消息;

- b) 报警被清除后，只能由操纵员直接通过报警控制和管理动作，而不是自动方法，重新排列或关闭在画面上显示的信息。

报警显示处理应基于系统的和一致的技术方法，以进行报警逻辑处理，这用于控制报警显示。

8.2 组合报警

组合报警可以用来从逻辑上组合几个用来表示单一信息或标识的报警信号，可以使用与、或、非和延时等逻辑。

每个单一报警信号宜关联到一个组报警，并且宜提供从组报警访问每个单一报警的方法。

只有那些纠正行动本质上相同的报警才可以组合成一组，组报警可以由下面几种情况组成：

- a) 冗余部件在相同条件下的报警，这些冗余部件有紧邻的、性质相似的独立指示仪表；
- b) 一个给定系统或部件的所有具有相同紧急或重要程度的报警；
- c) 一个系统中所有需要操作人员去现场进一步调查的报警；
- d) 控制室其他地方可用的单输入报警情况的综合报警。

8.3 报警抑制

8.3.1 抑制

报警可以通过报警显示处理自动抑制，或手动抑制。宜清楚定义自动抑制的准则。自动抑制的方法可包括：

- a) 减少已经在特定时间内显示并确认的持续报警状态；
- b) 降低对信息或状态的处理功能所产生报警的优先级别；
- c) 延时显示报警以便操纵员注意更重要的报警，如在报警雪崩时；
- d) 通过确认程序来鉴别有缺陷的报警信号，并用来抑制处理功能产生的相关报警；
- e) 抑制已经退出运行的设备相关的报警。

应通过报警选择或对抑制功能的鉴别要求，提供手动抑制报警的方式。

应提供手段，以能够对抑制的报警进行检查、记录、返回正常状态和确认。使用VDU的信息显示屏可有效实现这些功能。

在报警系统中表达的信息应一致，设计中应预防一个画面上的抑制报警同时在其他类似显示中显示相同报警，因为它属于运行中的不一致，可能引起操纵员对真实电厂状态的理解错误。

8.3.2 干扰报警

对于那些重复出现的干扰报警应允许操纵员抑制它们。在抑制后直到解除抑制前，报警信号不应引起任何画面变化，但它们的状态在操纵员需要时宜查看到。

8.3.3 持续报警

宜提供一种手段，将持续的报警从VDU的显示列表中移除，以避免显示列表中保留过多的报警。应允许操纵员选择一个报警或一组报警并将其移到持续报警列表中或其他记录这些报警的地方。但这些报警信号应仍具有可操作性，以便在报警消失或消失后又出现时，其状态可在画面中识别。

8.4 暗盘原则

在电厂满功率运行时宜做到无报警运行，在低功率时也推荐采用无报警运行方式。最基本的一个准则就是在满足安全性和可用性目标的条件下尽量减少报警数量。这个准则可以应用于报警盘、报警光字牌、大屏幕和VDU显示方式上。

9 报警控制和管理

9.1 概述

对于所有类型的报警显示（如报警盘、报警光字牌、VDU显示、大屏幕显示等），报警控制宜一致。报警控制器（如按钮、VDU菜单、鼠标点击目标等）之间应能容易区分开，如根据形状、颜色和小等，以便降低误操作的可能性。一般推荐下面的方式：

- a) 对消音、确认和复位宜提供独立的控制手段；
- b) 不同的报警控制宜采用不同的编码以便容易区分；
- c) 每一组报警控制，同一功能应在同一相对位置；
- d) 报警控制设计不宜允许操纵员闭锁该控制。

对任何显示方式的报警宜遵循同一个标准的报警控制顺序（如对报警盘和计算机化的报警显示方式）。

典型的报警控制和管理序列见图2和图3。

9.2 声音警告和消音

9.2.1 声音警告和消音逻辑

当一个报警刚开始显示时应提供一个声音警告直到被自动或手动消音或确认。如果报警消失后又重新出现，根据报警重新出现时间的间隔，声音警告也宜重新响起。

触发声音的逻辑设计应考虑到短时间内出现大量报警时不应影响操纵员。除了使用在预定的周期内自动消音功能外，不应使用手动报警静音功能。

9.2.2 声音编码

警告声音不应被可知的环境噪音掩盖并应可以很容易的从其他系统的声音信号（如电厂安全、辐射撤离警告、火警或类似的危害警告）中区分出来。通常认为这个声音应高于环境噪声10dB是合适的。该声音的大小宜在一定的范围内可以调节。

声音的大小和重复频率可以根据警告的重要性（如报警和事件通告）而不同。

可以采用操纵员可辨别的几种不同声音来表达报警的优先级。推荐在控制室采用不超过五种声音以免引起操纵员的混淆。

9.3 闪光和重闪

出现报警条件而触发报警时应产生一个闪光视觉信号。不推荐VDU上整条报警信息都闪光。

闪光频率可以是1Hz~5Hz。较快的闪光频率可以用于显示一个自动操作序列没有开始或正确中止。报警盘和报警光字牌的闪光时间宜与主控室范围内所有闪光状态同步。

重闪是一种自动化的报警管理功能，用于当报警被消除或确认后，重新出现时，再次产生一个报警信息。

对所有组报警都应有重闪功能。对一个组合报警当其中任何一个子报警信号改变到非安全状态时应重闪。

对VDU上的报警，当报警条件消失后但相关报警信息还在当前可见画面上（还保留在列表中但还未复位时），报警条件又重新出现时应重新闪光。否则应显示为一个新出的报警或在当前可见屏上通过一个提示语指示。

9.4 确认

对于每一组报警，如在一个报警盘上、一组报警光字牌，或相邻VDU上显示的报警，应提供一个确认控制功能。

在确认后报警应停止闪光并保持平光。确认可以直接触发消音动作。报警确认只能在相关报警对操纵员可见的地方进行。报警确认控制应不能对未显示出来的报警或隐藏在其他VDU显示格式后面的这些报警进行报警确认。

9.5 回铃

报警回铃是一种自动化的报警管理功能，它通过声音和/或视觉方式来通知操纵员报警已经消失并可以被复位。

报警回铃应用在应明确通知操纵员曾经是异常的条件已消失的重要地方。

在VDU上报警回铃功能应谨慎使用以免使得报警数量过多掩盖了其他报警。

9.6 复位

对于每一组报警，如一个报警盘上或一组报警光字牌，或相邻VDU上的报警，应提供复位控制功能。

报警复位应将相关的消失报警置于恰当的定义状态。如使报警光字牌的灯熄灭，从报警列表中移除相关消息或符号，或从图符旁移除相关标志等。

VDU上报警消息的复位处理应和报警盘上的报警处理一致。可以在当前浏览的报警信息页触发复位动作，或在当前浏览的整个报警列表中采取复位操作。复位动作应将已消失的报警消息删除，但在设计上应避免因此而引起已浏览页内容的大量改变。为了减小这种影响，对已浏览过的但不在当前页显示的报警，应在其可见时再移除。

与已复位报警相关的报警在继续存在的情况下仍应显示出来。

如果检查某个报警是否已消失对操纵员来说非常重要，则该报警应设计为需采取手动复位序列。如果操纵员需要响应大量报警或必需立即复位系统的报警，可以采用自动复位序列。

报警复位只能从电厂运行人员知道哪些报警将复位的地方进行。

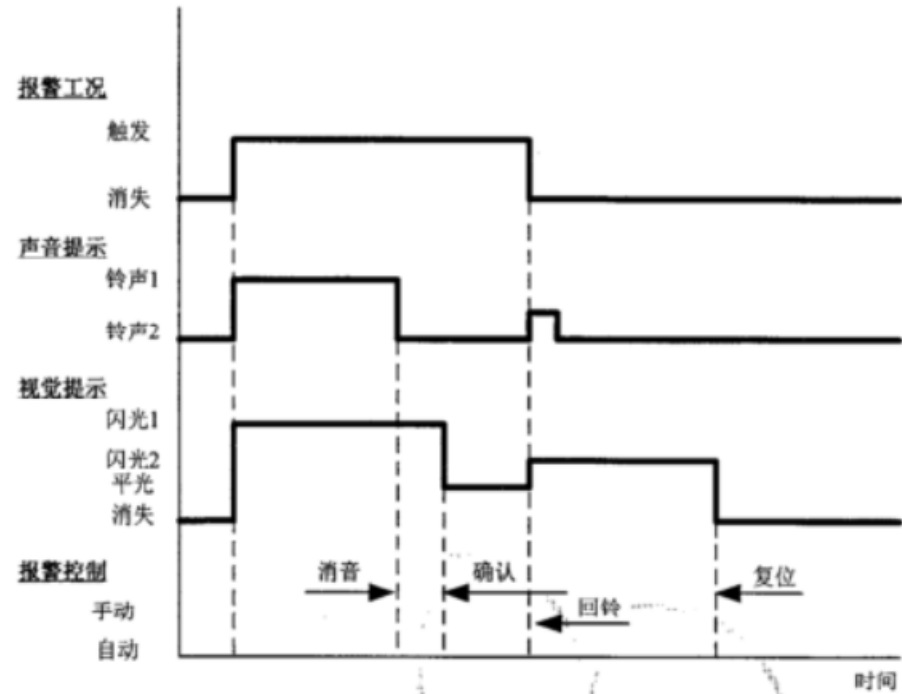
10 报警显示和显示—控制集成

10.1 概述

10.1.1 功能

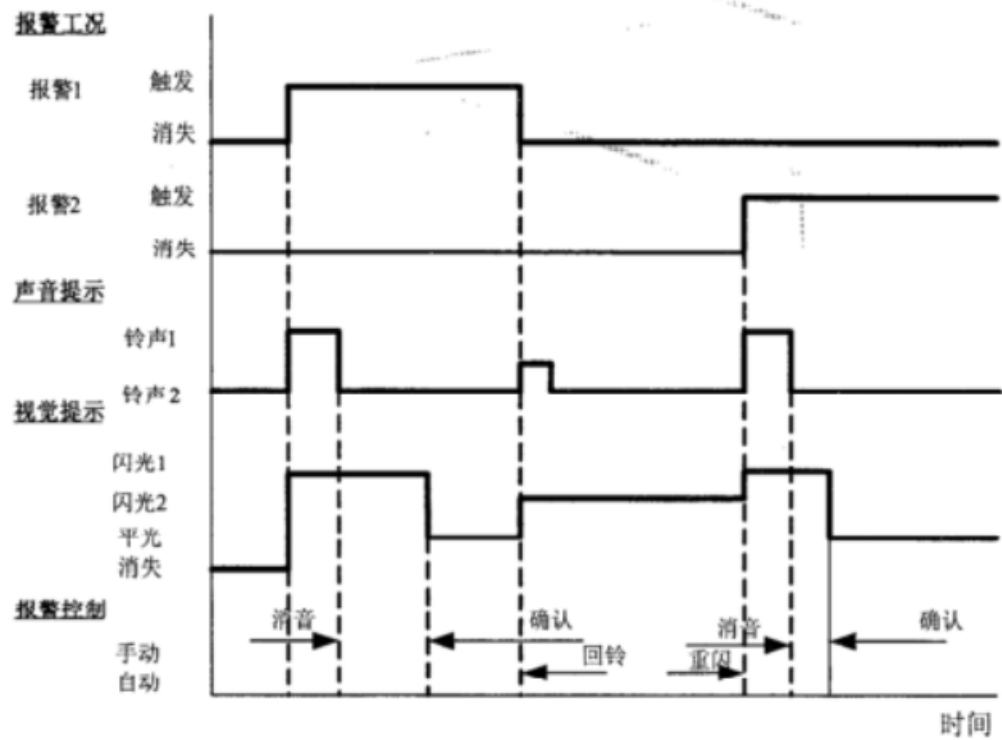
报警显示应通过报警信号和显示处理、布局、视觉和听觉方法来提供5.1到5.6所提到的报警功能。具体的说，报警显示功能宜：

- a) 清楚地指示出报警条件的存在；
- b) 在最开始通过声音警告和闪光（或VDU上闪光的标记）使操纵员注意到这种非正常情况并对其进行评估；
- c) 通过简单明了的信息恰当地描述这种非正常状态；
- d) 相关信息的显示应置于适当的环境和位置，以帮助操纵员评估和决策；
- e) 明确指出报警的状态（如新报警、已确认、已消失或被抑制）；
- f) 简单表示和其他报警或设备的关系；
- g) 帮助操纵员正确响应每个报警；
- h) 引导操纵员需要到其他显示设备上去验证或澄清该报警的状态；
- i) 支持所有运行人员保持对电厂状态及电厂主要功能的了解。



注：铃声1和铃声2可以相同；闪光1和闪光2可以相同。

图2 典型的报警控制顺序



注：报警1和报警2组合成一个组合报警。当报警2触发时，需要重闪。此例中，报警1消失后，没有执行复位操作。

图3 典型的组合报警控制顺序

10.1.2 基本显示方式的选择

在设计早期就应确定报警的基本显示方式，该方式应与5.1到5.6的功能目标一致。可以考虑下面的报警表示方式：

- a) 报警盘；
- b) 报警光字牌；
- c) 不一致指示器；
- d) 指示灯；
- e) 带查询功能的VDU显示；
- f) 大屏幕显示；
- g) 包括由计算机系统驱动的壁挂式显示盘台。

报警系统应尽可能按功能集成，特别是当它使用了不同的指示方式和置于主控室不同区域时（如VDU，大屏幕和专用盘台）。也就是说不应将两个（或更多）独立的子系统并排放在一起，除非是基于功能和操作集成上的考虑。

报警盘、报警光字牌和不一致指示器应允许使用暗盘原则。不一致指示器和指示灯可能比较特殊，不能满足暗盘原则。不一致灯用于指示那些在某些情况下是安全的但某些情况下非安全的操作，如启动是否正确或非期望的专设安全设施失效。许多电厂现在采用VDU来显示所有报警，除了少量在计算机失效的情况下仍要求可用的非常关键的报警。电厂也可能会有一个大模拟盘如大屏幕或带VDU和软控功能的壁挂式盘台来显示报警。

报警盘、大屏幕、壁挂式盘台和报警光字牌能同时以不同的方式有效的告知操纵员发生了什么，这有助于他们对异常的共同理解和认识，包括理解根据大量报警关系和传输位置来确定的异常。

VDU是用来完整显示相关信息的主要监测设备。它可以连续或在需要时显示报警，也可以在屏幕顶端或底端显示提示语，也可以按报警发生的时间排序进行显示。

这种通用或公用VDU工具可以和其他显示方式一起完成报警显示功能，大屏幕上的有效显示区域、几个位置的可用画面、VDU和报警盘的联合使用、大屏幕或其他方式可用于完成并行显示。

可以在计算机化的报警系统中集成报警盘和VDU显示器的全部特性并取二者之长。VDU显示在保证操纵员快速理解报警的限度范围内，允许对报警进行简单的重新整理和分组。

在通常情况下，主报警显示画面宜是VDU，使用VDU及补充使用报警盘和VDU可以有效给操纵员提供足够的信息。当采用VDU显示报警时，工艺流程图或模拟图上非常适合用符号或下翻式信息盘来显示报警信息。

10.1.3 布置

报警显示和报警消息的位置和种类应保证下述要求：

- a) 各类运行人员都有报警需求以执行其分配的任务；
- b) 对于整个电厂运行，所有运行人员都能看到必要的报警，这些报警可能是第6章定义的关键报警。

在不同的运行模式下（如正常和紧急模式下）运行人员构成和数量可能不同，在每种运行模式下都宜通过相关工作站访问报警画面。

报警显示的布置应符合主控制室总体设计原则。对于多机组控制室，报警显示的布置宜予特别考虑（例如，多个机组的有些报警是重复的）。

报警显示的布置应有助于操纵员通过显示设备上熟悉的位置来理解信息。

10.1.4 空间组合

组合的规则应清晰并和操纵员的使用习惯一致。

在控制盘上进行的实体上的报警组合或通过VDU显示方法进行的相关组合，宜给操纵员提供一个很容易鉴别受影响的功能或系统的方法。

按照形成控制室设计基准的功能方法（见IEC 61839），报警宜按电厂功能、可用性和安全功能在空间上进行组合，使得相关的所有报警在一个分组中。

其他按空间分组的可能方法还包括按电厂系统或逻辑结构组织报警，还可以进一步采用子组对报警进行组织。相关样例参见附录D。

10.1.5 报警标志和消息的格式

报警标志、消息或标题宜简单易懂，采用标准的术语并明确表达该报警的含义，以便于操纵员能读懂该消息。

报警标志和消息应唯一并清楚地表达受影响的电厂物项和故障点或工况的本质属性（如工艺参数、设备）。初始信号或继发信号的标记或一个唯一参考码宜是整个报警信息的一部分。

报警的名称宜在整个电厂的使用过程中保持一致。报警标志和消息格式对所有报警应保持一致。

报警标志或消息的描述宜遵循系统性顺序，这可以是主要的电厂分组及标识、次级的电厂分组及标识、条件或参数、异常状态。

核电厂中用来准确的辨别报警的报警标志可能会很长和详细，因而对报警光字牌和VDU显示器都会有一个报警消息的长度限制。受设备限制一般来说不应超过40个罗马字符（含空格），除非采用了双行显示模式。除非空间不够否则不宜采用缩写。如果一个标识或消息太长，在保证相关信息可以很容易理解的情况下可以采用缩写。如果采用了缩写，应基于系统化规则。

如下的系统性的缩写原则宜予指定和运用：

- a) 一些共同工况的缩写，如压力高，水位低；
- b) 电厂机组、序列、设备编码或其他缩写；
- c) 逐步缩短用于定义消息的常用单词，一个可行的方法是先不删除，然后删除一个，再删除两个参考单词的元音（适用于英文单词）。

对报警标识和报警消息的清晰和易理解性，宜在设计阶段由人因专家和电厂运行人员代表进行系统的审查。

10.1.6 显示编码

显示编码宜与电厂编码原则一致，并系统地应用于整个报警显示。

显示编码宜保证操纵员在任何运行工况下都能迅速的发现和理解报警。

报警编码（如快闪或点亮）宜用于要求要操纵员快速采取行动的报警。重要性可以通过颜色编码来表示。

例如，为了在大量报警出现时识别重要报警，可以采用有三种颜色的动态优先级显示。在任何点的重要报警可以显示为红色，其他信息可以用黄色或绿色。

当报警显示出来时，操纵员应能很容易的获得报警的优先级信息。对每一类重要优先级报警，可以在一个单独的VDU上显示。

10.2 报警盘和报警光字牌

10.2.1 报警标志

报警盘和报警光字牌的标志应满足 10.1.5的原则。

报警盘的标志应根据所有报警盘的标题进行分组，如根据所影响的电厂区域代码。这样就可以省略相关代码以缩短报警标识的长度。

对于模拟盘或类似布置的控制盘中集成的报警光字牌，可能通过模式或位置提示予以准确识别报警，可以使用如“压力高”这样的简短消息。

10.2.2 报警盘和报警光字牌的布置

报警盘面上的报警光字牌标识应易于识别，像通过窗口格局、颜色、分组、音频编码和分类报警等方式，旨在避免对状况的错误判断。

当许多报警出现时，为了更容易识别报警的重要等级，可以使用变化三种颜色的报警光字牌来表示动态优先级，这样可以避免报警被屏蔽，降低操纵员忽略报警或错误识别报警的几率。VDU显示方式宜用于组合报警显示、按时间顺序排序的报警显示和报警消息插播显示。

盘面显示方式可使用固定逻辑去识别最高级别的报警或者首出报警，让它显示在已经存在的分组中，而不影响那些已经存在于分组中的报警。

报警盘面和光字牌可以用来显示电厂的状态，指示电厂的可用性和运行的正确性。反应堆自动控制系统和安全系统的状态也可以通过报警盘和报警光字牌显示。当这些状态信息用来产生报警时，报警信号处理需要确定何时产生报警。更多的信息参见附录E。

10.3 VDU 报警列表画面

10.3.1 概述

对于采用基于计算机显示方式的电厂，利用VDU显示报警可以使报警显示方式和提供控制室需要的更多其他信息的显示画面一体化。这使得操纵员有了直接的途径从报警显示页面链接到电厂状态信息显示画面，协助操纵员诊断和决定适当的行动。

报警盘和报警光字牌显示的报警和组合报警也应显示在VDU画面上。设计时应考虑允许通过适当操作获取形成组合报警的报警信号的详细信息，例如在报警消息栏上使用光标和点击鼠标或触摸屏方式获取。

对于报警显示，例如VDU方式的报警消息列表，应提供足够的显示区域用于同时查看所有高优先级的报警，或者另一种方法是显示整体框架或允许高优先级报警的快速显示。或许空间固定显示方式或显示盘是最好的解决办法。报警列表需提供简单的滚动条或者翻页功能和快速显示最近报警的功能。

10.3.2 VDU 上的报警消息

VDU或大屏幕显示的报警消息应遵循10.1.5给出的规则。

VDU上的报警信息和打印方式下的报警信息应是一致的。为了防止操纵员混淆，需要提供一个缩略语清单并且可以从屏幕上调出。

屏幕上显示的按照某种顺序排列的报警（时间顺序显示）应表明每个报警触发和消除的时间，以允许与这个报警相关的其他显示形式（例如趋势曲线、事件日志）进行该报警的评价。

10.3.3 VDU 报警画面结构

使用VDU显示报警的方法应允许已经出现的报警按照时序记录来显示。这可以通过将新近出现的报警分成几页列表的形式来实现。最新页（也称首页）的报警，通常和刚刚出现的报警可在同一画面上，只是刚刚出现的报警在报警信息附近伴随有闪光标记。通过适当的控制操作可以将较前的报警页面显示出来。

报警列表宜有不同的方式来组合显示。通过适当的控制操作，如选择排列类型或者选择存储于计算机中的报警列表类型，能够显示各类报警列表。包含以下几种列表：

- a) 以时间顺序排列的报警，从全局到电厂细节的每一个显示层次；
- b) 每一个优先级层次的报警；
- c) 抑制的报警或没有运行意义的“干扰”报警；
- d) 从任一时间顺序排列的列表中移出的、操纵员知道并已确认出现了很长一段时间的报警；
- e) 与每个特定电厂项目相关联的，按标签特征顺序、基于电厂系统顺序或按时间顺序排序的报警；
- f) 在报警信号处理之前作为报警系统输入的报警信号；
- g) 特定类型的报警。

从首页溢出的报警可在后面的页面中显示。特别是，如果一个没有确认的报警包含在其他页面中，正好此页没有显示出来，这时应给出听觉和视觉指示如“自动插方式”以提请操纵员注意，在其他页面或画面上存在未经确认的报警。

基于计算机(控制)的VDU系统，可以利用后续的控制操作“保持画面”，用于显示“最后一个未确认报警”。该功能能在关键运行工况下防止画面自动更新，这样就可以让高优先级报警立刻显示，同时又保持了正常优先级报警快速自动显示的优势。

VDU报警画面应包含允许操纵员快速查看最重要报警和报警分组的结构，且通过画面找到电厂异常的具体信息。

VDU系统宜允许报警信号直接显示，报警信号经逻辑处理生成报警。此方法宜允许存在报警的任何部分都可以被识别，也宜与画面导航和整个电厂的显示方式结合起来。更多的信息见IEC 61772，并参见附录B。

VDU显示方法应提供人机查询画面。可能用到的方法如下：

- a) 鼠标或者光标点击组合报警信息，弹出窗口显示组合报警的组成；
- b) 点击一个显示值，弹出窗口显示报警阈值和信号状态；
- c) 点击一条报警消息，提供直接关联到电厂工况的画面导航；
- d) 点击一条报警消息，提供一个菜单并开始一个控制序列，例如：抑制干扰报警或持续报警或者将这些报警返回服役状态；
- e) 通过键盘输入搜索条件，例如选择报警标识，电厂设备或者仪表类型编码，给出所有相关联报警的打印输出。

除了鼠标和光标外，其他的选择方式或许会用到，例如用多位置开关、键盘或触摸屏来选择报警信息或相关的信号。

10.3.4 报警显示画面布局和格式

表征报警出现的简短的可视索引应在所有的VDU屏幕上显示，这些信息可能在每个屏幕的底部或者顶部显示。该类信息可能还包括出现报警的个数或者还没有确认的报警数量、查看报警的VDU屏幕标识或类似显示器。当报警被显示或者被确认，这些可视索引应以一个固定的时间来刷新，例如每秒一次。

为了避免相邻信息行间造成混乱，在VDU报警信息画面上每隔四行或五行插入一条分隔符（例如空行或者直线）。

10.3.5 控制

VDU报警的控制操作应和整个计算机系统的所有VDU控制结合起来。这些控制应充分、可靠、生命周期长、以及对电厂控制室环境是合适的。任何目标的控制序列应简短，适宜“一键”操作。合适的方法包括：

- a) 靠近每个VDU的硬件按钮和开关；

- b) 靠近每个 VDU 的标准的字母键盘或特殊设计的键盘;
- c) 滚动球、光标或者鼠标点击 VDU 画面上的菜单或者目标区域。

调出所需屏幕的操作次数应尽可能最小化,推荐两次或者更少操作。通过相关屏幕上请求按钮或其他控制方式的一次操作应也能够调出所需屏幕。画面设计导则见 IEC 61772。

10.4 音响报警

音响报警可能包括为了引起操纵员注意的语音通告,使他们不错过报警引起的事件通告。

语音是一种可接受的展现界面相关信息的媒介,联合使用语音展现报警信息有诸多优点。然而,单独使用语音展现报警信息不值得推荐。语音的广泛应用应尽量避免,因为这样会让操纵员分心或者厌烦。

11 可靠性,试验和可维修性

11.1 可靠性

集成报警系统的可靠性要求宜与报警功能安全重要性要求一致。系统单一故障不应导致报警多重失效。推荐采用适当的冗余和配置自诊断功能去探测系统的失效。

当报警出现在作为主显示的VDU上,操纵员应可以通过更多的VDU去访问该报警。

11.2 试验

每个报警应在报警系统安装后在现场进行试验,试验分别从报警系统设备终端和报警信号触发装置来进行。在电厂试运行前应确保所有的报警充分满足正常工作状态要求。

应提供一种对报警盘或者报警光字牌的光源进行试验的控制手段,包括对闪光功能进行试验的方法。

使用VDU方式显示的每一个报警在调试期间都应正常显示,包括准确的标题、逻辑处理和相关联的信息。或许可以通过交迭测试方式分别测试信号触发设备响应报警信号输入的正确性以及针对这些输入报警显示的正确性。

每一个与安全相关的重要报警都应在现场进行测试,测试从信号触发设备到报警的正确显示,且测试结果应予以保存。

在系统调试期间,应进行报警系统试验,以证明所有的报警信号处理和报警显示处理功能都能令人满意。需要完成一项针对短时间内出现大量报警信号的正确探测、存储和报警的产生与显示的试验(例如,一种合适的试验方法是通过仿真或信号注入方式在数秒内产生数百个报警信号,同时测试系统的输出。)

11.3 可维修性

报警系统应设计成其维修活动对操纵员影响最小化。将一个报警停役应考虑下述因素:

- a) 停役报警的指示,完全将报警停役会使与这个报警相关的视觉和听觉信号的产生源中止。此外,在报警系统设计中应考虑快速识别停役报警或加标签报警的提示设计。
- b) 报警系统故障指示:报警系统的故障信息应及时提供给操纵员,并且应给出报警系统故障位置或故障部件。

对于报警光字牌或者报警盘,应考虑下列因素:

- a) 平光时间延长,如果正常运行时由于设备维修或置换使得报警光字牌或报警盘应置于一个延期的‘点亮’状态,在这期间应使用合适的方式对这些报警光字牌加以明确标识,并且由行政管理程序来控制:

- b) 报警光字牌面盖的置换,如果灯置换时要求移除带有报警标识面盖,应用一种方法确保该报警标识面盖放回原处;
- c) 避免危险,灯置换应不引起电击危险;
- d) 在置换灯泡时,必要时,提供操纵员协助手段。

12 报警记录

为了便于以后分析,所有与安全相关的重要报警都会被记录。记录可能直接或者缓存后打印,又或采用合适的存储系统(例如磁盘、磁带或一次写入的光学媒介)用于显示或者打印,便于查询。应提供查询和选择记录的章节或特定的报警信号历史记录的工具。

状态改变的报警和报警信号记录应能够打印输出,被选择的电厂系统的报警和报警信号历史记录也应能够打印输出。

报警信息的记录应包括报警出现和消失的时间和顺序,以及其他开关量信号顺序和模拟量信号趋势。

一些电厂可能包括快速的事件顺序记录(SOE)系统,用于一个重要的电气故障发生后,识别并记录10ms内或者更快的开关装置事件。

13 报警响应规程(ARP)

13.1 概述

每个报警宜有ARP。

操纵员宜能够从读取报警信息的位置访问ARP。

ARP信息应与控制板上的信息一致,与报警系统、校准报警设定值的I&C程序、确定设定值的控制文件(例如,技术规格书和事故分析报告)和电厂其他程序及技术文件中相关信息一致。

13.2 内容

ARP宜包含以下信息:

- a) 报警在系统或功能中的分组;
- b) 正确的报警信息、正文或图例;
- c) 报警源(即发出信号的一个或多个传感器,包括报警信号处理或信号确认逻辑、驱动装置及附带的原理图,由此就能找到此设备);
- d) 报警阈值;
- e) 优先级(安全重要性);
- f) 报警可能的根本原因(例如,低水位-长期的给水不足);
- g) 需要操纵员立即采取的行动,包括操纵员确认报警存在条件的动作;
- h) 当报警发生时自动装置的动作(操纵员需要检查已经发生的动作);
- i) 后续的行动;
- j) 相关的参考;
- k) 确认报警原因所需的诊断提示;
- l) 电厂后续运行工况的指示。

13.3 格式

ARP的格式宜满足以下几点:

- a) ARP 的每一页应有合适的标识;
- b) 重要条目应有合适标识;
- c) 易于在每一页的相同位置查找信息的类别;
- d) ARP 的全部信息的显示应一致;
- e) 操纵员获取信息所需的后翻和前翻动作应最简化。

附录 A
(资料性附录)
报警系统问题

本附录给出的例子是基于实践经验。

A.1 正常和雪崩时报警和信息变化率

在一个核电厂中触发报警的信息信号出现的正常变化率能达到每天变化几百个,报警系统通常都能处理。在电厂脱扣和大的瞬态时,产生报警的输入信息信号快速的变化触发更多的信号,以“雪崩”或“洪水”式的变化。没有运用合适逻辑的电厂,在记忆和处理这种信息流方面已有对付问题的经历。在这些情况下,如果不从信息中对报警进行仔细的取舍,电厂依然会存在信息相对于操纵员超负荷的问题。

事实表明,操纵员读取一个VDU报警信息不可能快于10s,对出现的每个报警的含义进行分析会需要更长的时间(几分钟)。因此,报警产生过程的设计,要便于识别需采取积极行动的报警,即使在触发报警的输入信息迅速变化的情况下,它们的表达方式也不超出操纵员的理解能力。

在多数反应堆、电厂或电气保护动作的情况下,核电厂出现了几秒钟约1000次的信息变化速率。在保护动作发生后一小时内,信息更迭频率逐渐降低到每分钟200多次,或每分钟数次,或数分钟一次。

信息和报警变化的分辨率对于一般电厂报警200ms是合适的,但是对于特殊的开关装置事件顺序记录(SOE)系统要求低于10ms的分辨率。

A.2 干扰报警

在基于计算机报警系统中,电厂经历的问题归咎于故障的初始信号、不正确的阈值或者回差设置,这些原因导致报警反复产生和消除。这些干扰信号的变化以10s至10min的典型间隔出现。研究信号变化的日志可以分辨出问题所在。维修有缺陷的设备触点并校正阈值信号和它们的滞后作用,就可以减少这类问题。用这些来降低干扰信号对操纵员的压力有时是不够的。对基于计算机的系统,在干扰源被修正后,抑制、记录这些报警并将它们恢复到服役状态的方法往往是必要且相对简单易行的。

附 录 B
(资料性附录)
触发报警的信号源

报警输入信号经过报警信号处理逻辑处理后产生报警信号,用于报警显示处理,这些报警输入信号来自核电厂的下列信号源:

- a) 接点信号,例如继电器或开关的辅助触点、限位开关;
- b) 固态逻辑输出、探测器、阀门状态、温度开关;
- c) 模拟信号与它的高限值或低限值(也就是带滞回特性的整定值)进行比较的结果;
- d) 控制和选择开关位置、自动/手动选择器确定的信息;
- e) 由安全系统或其他逻辑信号处理的安全和保护系统状态,处理方式取决于中子注量率水平、逻辑符合和运行状态;
- f) 为了探测异常状态的模拟信号计算,例如,某个堆芯出口温度与邻近通道的温度相比超过限值;
- g) 为了探测异常状态,使用模拟信号和状态信号的计算,例如,一个控制棒与该控制棒组位置不符的探测;
- h) 由电厂工况直接或间接引起的计算机处理状态或逻辑状态;
- i) 对状态和报警信号进行分组或逻辑处理产生的其他报警。

包含一座反应堆和汽轮机的典型核电机组,可能有大约10 000个模拟信号及至少10 000个接点和双态信号,可能产生至少20 000个报警信息。

附录 C

(资料性附录)

报警处理逻辑和动态优先级举例

C.1 报警逻辑处理方法

已经成功使用的方法包含如下：

- a) 安全系统报警的逻辑可能已经定义，安全系统报警的每一个冗余设置都可以同时出现。简单的分组逻辑可以有效运用。用低、中功率水平的闭锁、保护或者 ESF 需求、保护或 ESF 触发信号与其他信号一起，对更复杂的条件逻辑进行定义从而生成一个连续的运行模式。一些电厂已经使用由操纵员切换到定义运行模式的逻辑。利用这种运行模式，由配套的布尔逻辑来控制报警抑制和安全系统的报警分配以及其他报警画面。已开发类似的带有时间标签的分组逻辑，用于识别反应堆事故停堆工况和冗余安全设备的运行、识别电厂本应启动而实际还未启动的情况。
- b) 报警逻辑可以用在软件中实现的标准的逻辑门（与、或、非、定时器等）定义，以过滤报警，并通过假设电厂状态（从停闭到满功率）和报警条件确定哪些报警要被显示或抑制及其优先级如何。应以动态的方式考虑逻辑而不限于静态的条件，以便任何时间存在的报警的变化或预期出现的报警的失效，都将会生成一致的条件供逻辑抉择。
- c) 报警逻辑基于两个共存报警的相对重要性，重要性的判断从设计和现场经验得出。当报警出现时，计算机用关联报警数据库来检查与新报警相关的报警。如果没有相关联的报警存在，新报警分级为重要并以高优先级或高重要性显示出来；如果相关联的报警已经存在且先前已经显示出来，那么新报警分级为低重要性，不显示为报警只作为信息。

基于软件定时器，可以开发逻辑，用以控制由于电厂或电气保护动作带来的报警雪崩。

C.2 动态优先级

C.2.1 因果关系优先级

定义为主要原因的报警认为其具有更高优先级。

例如，如果泵跳闸保护触发了泵跳闸报警、失去流量报警、低水位报警，泵跳闸报警认为是更高优先级的报警，因为这个报警是根本原因，其他的报警都是由它引发。

因果方案有它的不利之处，相对于原因，操纵员可能更关注应补偿的后果。因此，正确选择后果报警优先级取决于操纵员预期执行的命令和动作的类型。如果主要动作是纠正故障原因且根本原因能清楚确定，则更高的优先级应赋予根本原因报警。此时或许抑制后果报警比降低它的优先级更合适。

C.2.2 严重程度优先级—多阈值报警

对于有多个报警阈值的参数，指示最严重情况的报警，具有更高优先级。

例如，低低报警比低报警有更高的优先级。

C.2.3 信息内容优先级

一些动作（例如停堆）的自然结果及显示对应设备状态的报警所提供的状态信息是正常的（例如预计偏差）而不作为异常（例如非计划偏差）报警考虑。它们可以被认为是较低优先级而不宜作为真实报警。

附录 D
(资料性附录)
报警分组和分类概念举例

与一般通过一组应控制的功能对电厂本身进行分析和描述(见IEC 61839)时,为了反映产生电能的总体设计准则,同时确保物理过程的安全特性,要用一个一致的报警系统结构层次来组织报警,以便反映电厂的功能体系。

因此报警能按由电厂功能进行分组,更进一步,再按过程、系统、部件等进行分组,从而建立一个优先和(或)表达的层次:

电厂功能—工艺过程—系统—部件—部件支持。

这种层级允许操纵员区分几类报警:

- a) 有关背离电厂功能主要目标的信息;
- b) 与控制该功能的工艺机械装置的相关干扰信息;
- c) 用以提供上述装置的实体系统内的异常信息;
- d) 有关那些系统设备部件失效的信息;
- e) 有关辅助系统故障的信息。

最高级别的报警分组涉及到电厂功能,压水堆核电厂一些典型的控制功能,例如:

- a) 反应性控制;
- b) 反应堆冷却剂装量控制;
- c) 汽轮机控制;
- d) 配电控制,等。

每个电厂功能都是通过几个工艺设备的动作来控制的,例如反应堆压力的变化能通过改变反应堆温度或者改变稳压器中反应堆水量或改变稳压器蒸汽与水的比率等来实现。依上所述,这是按工艺过程组织报警,属第二个层次。

通常由一个或者更多的实体系统,提供控制手段来管理这样的工艺过程,例如,一回路系统补水,可以根据具体情况,由反应堆补水系统或者安注系统来实现。根据上面指定的结构类型,这是按系统组织报警,属第三个层次。

在每一个实体系统内,都有许多设备(泵、加热器、阀门、风机等)在运行,以达到系统的期望目标;这些设备的运转受到辅助系统的支持,保证其部件的正常性能(例如电源、压缩空气、冷却水等的可用性)。按设备及其支持系统这两个领域组织报警,属于更下层的层次。

以这种方式得出的报警系统结构布局,使操纵员得以在非常有意义的报警环境下观测异常工况,减少筛选、整合重要信息并得出结果的工作负荷。例如,如果一个辅助系统的动作,由于某些原因背离了期望的行为,这样操纵员(通过适当的报警显示)就能够在特定设备运行的报警环境下,了解相关干扰具体属于哪一个系统,其支持某一特殊电厂功能必要的控制过程的执行。

同时,当报警触发时,操纵员一眼就能发现(如果显示结构恰当的话),哪些电厂功能是该过程扰动的目标(例如反应堆冷却剂压力控制:压力非正常降低);然后他(她)就能知道哪一个实体系统引起这个异常(例如稳压器系统),最终哪些设备和(或)辅助系统受到影响(例如,稳压器卸压阀XXYY泄露)。由于原始的分组,在显示选择的帮助下,操纵员可以很快得到越来越多的有意义的信息。

附录 E

(资料性附录)

区别报警和状态信息所需的素材

通常由报警系统表达的三种不同类型的电厂过程数据：

- a) 关于报警和异常的数据（真实报警信息尽可能准确表述异常的本质）；
- b) 关于自动系统（控制和保护系统）做什么的数据（如：安注启动 - 这不是异常工况，因为安注设计成在某些情形下介入；同样，有些情况下它的运行是正常的，即所期望的）；
- c) 关于复杂系统稳态的数据（如安全系统预运行准备就绪到运行）。这些信息也不是指出异常状况，仅为操纵员在不同工况下操作时进行信息确认而设计（正常）。

依据上述区别，报警系统代表性地提供两类信息：

- a) 非预期状态的信息；
- b) 预期状态的信息。

这两种类型的信息应考虑清楚，因为他们互为补充：异常信息的显示和不包含异常信息的显示，只是指出一些重要系统的状态；在传统主控室第二种类型信息通常纳入报警，这是因为，如安全系统的干预，会关系到故障的发生。状态信息的信息内容对操纵员来说也是很重要的，但该功能无法确切说出其来自于报警系统。因此，报警系统设计的第一要求如下：

这个要求的目标是充分遵守暗盘准则，这就要求电厂正常运行时，所有系统都在期望的配置下，报警显示盘是暗的（没有报警信息显示）。这一概念应用的失败可能引起操纵员任务超负荷。

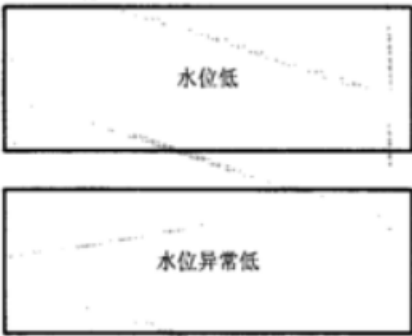
附录 F
(资料性附录)
报警光字牌排列样例

报警光字牌通常放置于面板的最上端。
同一系统的相似报警从左至右按字母顺序排列，见图F. 1。



图F. 1 冗余部件报警光字牌的水平排列方式

同一系统内报警进展的显示按照高低、上下从顶部到底部排列。如果与这种情况不符，更高级别的重要报警要置于顶部，见图F. 2。



图F. 2 不同重要性报警光字牌的竖向排列方法

如果属同一系统且正常使用程度相同的报警的传送元件因参数不同而变化，需要进行排列，原则上，从顶部到底部依次是压力、水位、温度和流量。

附 录 G
(资料性附录)
报警分类考虑要点举例

在IEC 61226中,报警一般属于C类或者不分类。然而,一些报警可以归类于更高级别。

报警分类可考虑如下因素:

- a) 有一些报警针对安全所需的不常出现的工况。宜考虑操纵员动作的响应时间;
 - b) 有一些报警在自动保护动作后需要一些手动操作以确保成功停堆。宜考虑操纵员动作响应的时
间;
 - c) 有一些报警用于警告安全系统、专设安全设施(ESF)或其支持系统部分不可用或故障,或没
按要求运行的情况;
 - d) 有一些报警旨在维持安全或减少反应堆故障频率,例如,控制正常功率工况的自动控制系统报
警、紧急或停堆时给水控制的报警;
 - e) 有一些报警警告工艺对人员的危害或放射性释放,例如从主控制室采暖和通风系统或环境监测
系统来的报警;
 - f) 在任何紧急停堆或故障后宜记录报警以供分析;
 - g) 核岛及其供电系统相关的大多数报警与反应堆安全没有直接的联系,但是它们与减少反应堆故
障频率有关;
 - h) 常规岛及其供电系统报警、电气系统报警与发电有关,通常和反应堆安全没有关系,但这些都
在设计时宜予考虑。
-

中 华 人 民 共 和 国
能 源 行 业 标 准
核电厂主控制室的报警功能与显示
NB/T 20027-2010

*

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

*

2010 年 10 月第 1 版 2010 年 10 月第 1 次印刷
印数 1—200