ICS 25.040
CCS N 19

中华人民共和国国家标准

GB/T 41261—2022/IEC 62682:2014

过程工业报警系统管理

Management of alarms systems for the process industries

（IEC 62682:2014,IDT）

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。

本文件等同采用IEC 62682:2014《过程工业报警系统管理》。

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。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位:机械工业仪器仪表综合技术经济研究所、国家管网集团西南管道有限责任公司、中国石油集团安全环保技术研究院有限公司、中国石油化工股份有限公司青岛安全工程研究院、山东省蓬渤安全环保服务有限公司、浙江中控技术股份有限公司、中国石油天然气管道工程有限公司、深圳市标利科技开发有限公司。

本文件主要起草人:刘瑶、魏海洋、朱明露、史学玲、朱建平、魏振强、徐德腾、帅冰、陈小华、卜志军、张雪、孙文勇、李玉明、孙舒、朱杰、张占峰、赵宇宁、杨柳、施隋靖、李秋娟、陈汝、孙腾、朱旭营、徐伟、王春利、王刚、熊文泽、张亚彬、牛蕴。

引　言

目的

本文件针对过程工业报警系统的开发、设计、安装和管理。报警管理包括报警系统全生命周期中的数个工作流程。本文件定义了开发报警系统的术语和模型，并提出了在全生命周期中有效维护报警系统所推荐的工作流程。

本文件源自 ANSI/ISA -18.2—2009，《过程工业报警系统管理》是一份国际自动化学会(ISA)标准，同时适当参考了行业中制定的其他指导文件。在重大过程事故调查报告中，无效的报警系统常常被认为是造成事故的影响因素。本文件旨在提供一套可以提高过程工业安全性的方法。

有效报警系统的相关术语和实践并非在本文件中首次定义。1999 年，工程设备和材料用户协会(EEMUA)发布了 191 版出版物：报警系统设计、管理和采购指南。2003 年，化工和制药工业过程控制技术用户协会(NAMUR)发布了工作表 NA 102：报警管理。

在制定本文件过程中，我们尽可能与这些组织和委员会前期工作中所使用的术语和实践保持一致。

本文件规定了报警管理和报警系统的相关要求。旨在为以下相关个人和组织提供指导：

a) 制造或实施嵌入式报警系统；

b) 制造或实施第三方报警系统软件；

c) 设计或安装报警系统；

d) 操作和/或维护报警系统；及

e) 审查或评估报警系统的性能。

组织机构

本文件包括两部分。第一部分是一般性介绍(第 1 章～第 5 章)，其后(第 6 章～第 18 章)是本文件的主体部分。

过程工业报警系统管理

1 范围

1.1 适用范围

本文件规定了过程工业设施报警系统生命周期管理的一般原则和流程，该报警系统基于可编程电子控制器和基于计算机的人机界面(HMI)技术。它涵盖了所有向操作员发出的报警，包括基本过程控制系统、警报器面板、安全仪表系统、火气系统以及应急响应系统的报警。

本文件中的实践方法适用于连续、批量和离散过程。

本文件在实施过程中可以存在差异，以满足不同工艺过程的特定需求。

除了本文件的要求外，还应遵循政府(如国家、省、市、自治州)制定的过程安全设计、过程安全管理或其他要求。

报警系统的主要功能是将异常工况或设备故障通知操作员，并支持其做出响应。报警系统既涉及基本过程控制系统(BPCS)，也涉及安全仪表系统(SIS)，每个系统都根据过程状况测量值和逻辑生成报警。图1展示了报警系统报警和响应数据流的概念。报警系统还包括一种通过人机界面向操作员发出报警信息的机制，通常是计算机屏幕或信号面板(光字牌)。报警系统的附加功能是报警和事件日志、报警历史记录，以及生成报警系统的性能指标。其他外部系统可使用报警系统数据。

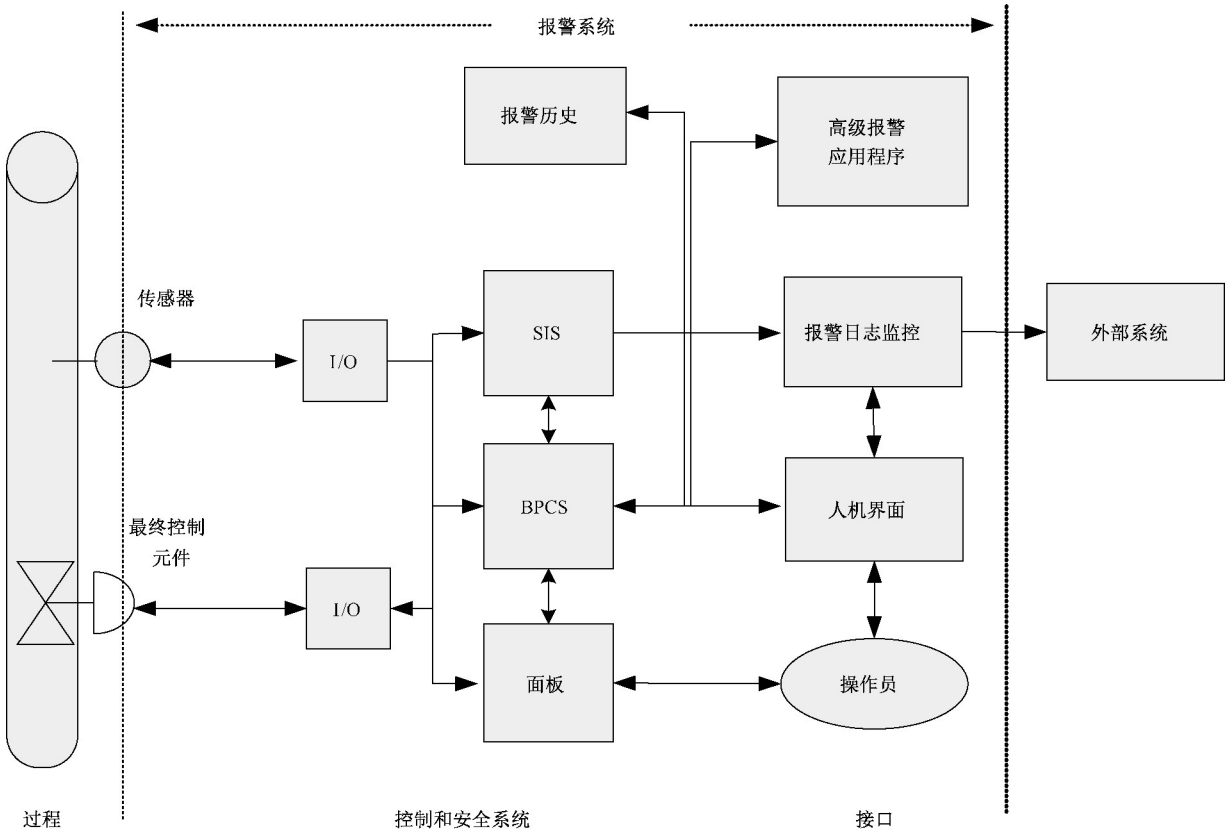


图 1 报警系统数据流

1.2 包含和排除

1.2.1 操作员

本文件范围包括操作员接收和响应报警功能。但操作员管理不在本文件范围中。

1.2.2 过程传感器和最终控制元件

传感器和最终控制元件发出的报警属于本文件范围。过程传感器和最终控制元件在图1中标示为执行报警的设备。过程传感器和最终控制元件的设计和管理不属于本文件范围。

1.2.3 安全仪表系统

安全仪表系统发出的报警属于本文件范围。安全仪表系统(SIS)在图1中标示为执行报警的设备。安全仪表系统的设计和管理不属于本文件范围。详细信息请参考GB/T 21109(所有部分)。

通过控制系统提供给操作员的来自火灾探测和保护系统或安保系统的报警和诊断属于本文件范围。火灾探测和保护系统以及安保系统不属于本文件范围。

1.2.4 事件数据

除了报警信号以外,模拟、离散和事件数据的指示和处理均不在本文件范围内。使用报警和事件数据的分析技术也不在本文件范围内。

1.2.5 报警识别方法

本文件中没有规定必要的报警识别方法。仅列举了数个报警识别方法的实例。

1.2.6 变更管理

本文件没有规定变更管理程序,但提供了变更管理程序的一些要求和建议。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义及缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

定值报警(阈值报警) absolute alarm

报警设定值为某一定值,当超过此定值时发出的报警。

3.1.2

确认 acknowledge

操作员证实收到报警的动作。

3.1.3

触发状态　active

报警处于报警条件为“真”的状态。

3.1.4

自适应报警　adaptive alarm

通过算法改变设定值的报警(如:基于比率)。

3.1.5

可调节报警　adjustable alarm

操作员设置报警　operator-set alarm

可以由操作员手动更改设定值的报警。

3.1.6

高级报警技术　advanced alarming

有助于在特定情况下管理警报的技术集。

示例:基于状态的报警技术。

3.1.7

报警　alarm

通过声音和/或可视的手段向操作员指示需要及时响应的设备故障、过程偏差或其他异常情况。

3.1.8

警报　annunciation

报警警报　alarm annunciation

报警系统的功能——使操作员注意到某个报警。

3.1.9

报警属性　alarm attribute

过程控制系统的报警属性设置。

示例:报警设定值。

3.1.10

报警分类　alarm class

具有相同报警管理要求(例如:测试、培训、监视和审查要求)的报警组审查。

示例:安全相关报警。

3.1.11

报警死区　alarm deadband

报警设定值与报警退出值之间的回差。

3.1.12

(报警)过滤　(alarm) filtering

根据报警记录的一个给定要素选择需要显示的报警记录的功能。

3.1.13

报警泛滥　alarm flood

在此情况下,报警率超过操作员可以有效管理的范围(例如:每 10 min 超过十次报警)。

3.1.14

报警组　alarm group

具有相关性的一组报警(例如:同一过程单元、过程区域、设备组或者服务)。

3.1.15

报警历史　alarm historian

报警记录的长期存储。

3.1.16

报警日志　alarm log

报警记录的短期存储。

3.1.17

报警管理　alarm management

报警系统管理　alarm system management

确定、记录、设计、操作、监视和维护报警系统的流程和实践。

3.1.18

报警信息　alarm message

报警时显示的文本字符串，为操作员提供附加信息（例如：操作员动作）。

3.1.19

报警解除延迟　alarm off-delay

去抖动　debounce

过程测量恢复到正常状态至报警解除的时间延迟。

3.1.20

报警延迟　alarm on-delay

过程测量达到报警状态到警报发出的时间延迟。

3.1.21

报警原则　alarm philosophy

用于建立设计、实施和维护一个报警系统的基本定义、原则和流程的文件。

3.1.22

报警优先级　alarm priority

在报警系统中为各报警分配的相对重要性，以表明需要响应的紧迫性（例如：后果的严重性和允许的响应时间）。

3.1.23

报警率　alarm rate

每位操作员在特定的时间间隔内接收的警报次数。

3.1.24

（报警）记录　（alarm）record

记录报警状态变化的一组信息。

3.1.25

报警设定值　alarm setpoint

报警限值　alarm limit

报警触发值　alarm trip point

触发报警的过程变量或离散状态的阈值。

3.1.26

（报警）排序　（alarm）sorting

根据报警记录的给定要素，调整报警记录显示顺序的功能。

3.1.27

报警汇总　alarm summary

报警列表　alarm list

按所选择信息(例如:日期、时间、优先级和报警类型)列出报警的展示列表。

注:报警汇总也可以显示已恢复正常的指示。

3.1.28

报警系统　alarm system

为应对异常工况,用于生成和处理报警的操作员支持系统。

注:报警系统包括操作员,见图1。

3.1.29

报警系统要求规范　alarm system requirements specification

规定报警系统设计详细要求的文件。

3.1.30

报警类型　alarm type

指示报警条件差异的报警属性。

示例:过程变量低报警、过程变量高报警或状态偏差报警。

3.1.31

警示　alert

通过有声和/或可视方法,提示操作员在时间允许时需要进行评估的设备或工况。

3.1.32

允许的响应时间　allowable response time

从报警发出到操作员采取纠正措施以避免发生不良后果之间的最大时间间隔。

3.1.33

通告器　annunciator

提示过程条件发生改变的设备或设备组。

3.1.34

评估　assessment

将通过监测和附加的定性(凭经验的)测量获得的信息与既定目标和确定的性能指标进行比较。

3.1.35

审查　audit

包括报警系统性能评价和报警系统管理工作实践效果的综合评估。

3.1.36

坏值报警　bad-measurement alarm

过程测量值超过预期范围时生成的报警(例如:4 mA～20 mA信号,如果测量值为3.8 mA,则发出报警)。

3.1.37

基准　benchmark

报警系统的初步审查,专用于识别问题区域,以便制定提升计划。

3.1.38

位模式报警　bit-pattern alarm

当数字信号与预先确定的模式相匹配时生成的报警。

3.1.39

计算报警　calculated alarm

通过计算值而不是直接过程测量值生成的报警。

3.1.40

呼叫报警　call-out alarm

控制台显示之外的,或作为控制台显示的补充手段的其他通知操作员的报警方式(例如:寻呼机或者电话)。

3.1.41

抖动报警　chattering alarm

短期内在报警状态和正常状态之间重复转换的报警。

3.1.42

分类　classification

基于共同要求(例如:测试、培训、监测和审查要求)将报警分为不同报警类别的过程。

3.1.43

控制系统　control system

对来自受控设备和/或操作员的输入信号进行响应,生成使受控设备按预期方式运行的输出信号的系统。

注:控制系统可能包括基本过程控制系统(BPCS)和安全仪表系统(SIS)。

3.1.44

控制器输出报警　controller-output alarm

由控制算法(例如:PID 控制器)的输出信号而非直接过程测量生成的报警。

3.1.45

停用　decommission

将报警从报警系统中移除的过程。

3.1.46

偏差报警　deviation alarm

当两个值的偏差超过限值(例如,冗余仪表之间的偏差或者过程变量和设定值之间的偏差)时生成的报警。

3.1.47

状态偏差报警　discrepancy alarm

不匹配报警　mismatch alarm

装置或设备的预期状态与实际状态之间出现差异时生成的报警(例如:要求启动后,电机无法启动。)

3.1.48

显示　display

将操作员监测的信息可视化。

3.1.49

动态报警　dynamic alarming

根据过程状态或条件自动修改报警属性。

3.1.50

强制　enforcement

可以验证并将控制系统中报警属性恢复至主报警数据库中设定数值的增强级报警技术。

3.1.51

事件　event

表示状态改变的事实(请求的或主动的)的表述。

注：例如模式变化或设备状态改变。

[来源：IEC 62264-2:2004,3.1.2,修改——增加注释]

3.1.52

瞬时报警　fleeting alarm

短时间内在触发状态和非触发状态之间切换的报警。

3.1.53

首出报警　first-out alarm

首要报警　first-up alarm

在多重报警场景下被确定(通过首出逻辑)最先发出的报警。

3.1.54

高级别管理报警　highly managed alarm

超过一般报警的带有附加要求的报警类别。

例如：安全报警。

3.1.55

人机界面　human machine interface;HMI

操作员所使用的硬件和软件集，以监测并与控制系统产生交互作用，从而通过控制系统与过程产生交互作用。

3.1.56

实施　implementation

设计和运行之间的过渡阶段，在此阶段报警投运。

注：实施包括诸如调试和培训等活动。

3.1.57

仪表诊断报警　instrument diagnostic alarm

现场设备生成的故障报警(例如：传感器失效)。

3.1.58

临时报警　interim alarm

临时使用的报警，以替代停用报警。

3.1.59

报警锁定　latching alarm

在过程条件恢复正常之后，仍处于报警状态，需要操作员进行复位才能将报警恢复到正常。

3.1.60

主报警数据库　master alarm database

经批准的合理化报警和相关属性列表。

3.1.61

监测　monitoring

报警系统性能的定量(客观)测量和报告。

3.1.62

滋扰报警　nuisance alarm

不必要的、过度的或在操作员做出响应之后无法恢复到正常状态的报警。

注：抖动报警、瞬时报警或陈旧报警。

3.1.63

操作员　operator

控制人员　controller

负责监视和改变过程的人员。

3.1.64

(操作员)控制台　(operator) console

用于操作员监视和/或控制过程的界面，可以包括多个显示器或警报器，并且定义操作员的控制范围的边界。

3.1.65

操作员站　operator station

操作员控制台中的人机界面。

注：操作员站可以包括多个屏幕。

3.1.66

停用状态　out-of-service

报警的一个状态，在此状态下报警指示被禁止(通常通过手动禁止)，例如为了维保。

3.1.67

装置状态　plant state

装置模式　plant mode

为过程装置定义的一套操作条件。

示例：停车或正常运行。

3.1.68

优先级分配　prioritization

为报警分配运行重要性级别的过程。

3.1.69

过程区域　process area

由现场确定的物理的、地理的或逻辑的资源分组。

[来源：IEC 62264-1:2003，3.1]

3.1.70

变化率报警　rate-of-change alarm

单位时间内过程变量变化($\mathrm{d}PV/\mathrm{d}t$)超过确定的设定值时发出的报警。

3.1.71

合理化　rationalization

使用报警原则检查潜在报警，为设计选择报警，并记录每个报警的基本原理的过程。

3.1.72

重新报警的报警　re-alarming alarm

重新触发报警　re-triggering alarm

在一定条件下自动向操作员重新发出警报的报警。

3.1.73

方案驱动的报警　recipe-driven alarm

设定值取决于当前正在执行方案的报警。

3.1.74

远程报警　remote alarm

来自远程操作的设备的报警，或向远程接口发出的报警。

3.1.75

重置　reset

操作员解锁被锁定报警的操作。

3.1.76

恢复正常　return to normal

解除　clear

报警从激活的警报状态到未激活的警报状态的转换。

3.1.77

安全仪表系统　safety instrumented system

用于实现一个或多个安全仪表功能的仪表系统。一个安全仪表系统由传感器、逻辑解算器和执行单元的任意组合组成。

注：这可以包括安全仪表控制功能或安全仪表保护功能或两者兼而有之。

[来源：GB/T 21109.1—2007，3.2.72]

3.1.78

安全相关报警　safety related alarm

安全报警　safety alarm

被分类为对过程安全（保护人员生命和环境）至关重要的报警。

示例：风险降低因子大于 10 的报警。

3.1.79

报警搁置　shelve

由操作员发起的临时性报警抑制，有工程控制手段解除报警抑制。

3.1.80

静音　silence

操作员终止有声报警的操作。

3.1.81

陈旧报警　stale alarm

警报持续时间过长的报警（例如：24 h）。

3.1.82

基于状态的报警　state-based alarm

基于模式的报警　mode-based alarms

可根据运行状态或过程条件对其进行属性修改或进行抑制的报警。

3.1.83

统计报警　statistical alarm

基于对一个或多个过程变量的统计处理而生成的报警。

3.1.84

报警抑制　suppress

当报警被激活时，防止其向操作员发出报警警示。

示例：搁置、抑制设计、摘除。

3.1.85

依据设计抑制　suppressed by design

根据装置状态或其他条件防止向操作员发出报警警示。

3.1.86

系统诊断报警　system diagnostic alarm

由控制系统发出的报警，提示系统硬件、软件或组件发生故障。

示例：通信错误。

3.1.87

标签　tag

点　point

分配给控制系统中的过程测量、计算或设备的唯一标识符。

3.1.88

未确认的　unacknowledged

操作员对收到的报警指示尚未确认的报警状态。

3.2　缩略语

下列缩略语适用于本文件。

ACKED：已确认（Acknowledged）

ASRS：报警系统要求规范（Alarm System Requirements Specification）

BPCS：基本过程控制系统（Basic Process Control System）

cGMP：现行良好生产实践（Current Good Manufacturing Practice）

DSUPR：设计抑制（Designed Suppression）

EEMUA：工程设备和材料用户协会（Engineering Equipment and Materials Users'Association）

ERP：企业资源规划（Enterprise Resource Planning）

FMEA：故障模式和影响分析（Failure Mode and Effects Analysis）

HAZOP：危险与可操作性分析（Hazard and Operability Study）

HMA：高级别管理报警（Highly Managed Alarms）

HMI：人机界面（Human Machine Interface）

I/O：输入/输出（Input/Output）

LOPA：保护层分析（Layer of Protection Analysis）

MES：制造执行系统（Manufacturing Execution System）

MOC：变更管理（Management of Change）

NORM：正常（Normal）

OOSRV：停用（Out of Service）

P&ID：管道（或过程）和仪表图[Piping (or Process) and Instrumentation Diagram]

PHA：工艺危险分析（Process Hazards Analysis）

RTNUN：未确认但已恢复正常（Return to Normal Unacknowledged）

SHLVD：搁置（Shelved）

SIS：安全仪表系统（Safety Instrumented System）

SOP：标准操作程序（Standard Operating Procedure）

SRS：安全要求规范（Safety Requirement Specification）

UNACK:未确认(Unacknowledged)

4 标准符合性

4.1 一致性指导

为符合本文件,规范条款的每项要求均需获得满足。业主/经营者需对此负责。

4.2 现有系统

针对本文件颁布之前按照其他规范、标准和/或实践进行设计和构建的现有报警系统,业主/运营者应当确定设备设计、维护、检查、测试和运行的安全性。

本文件的实践和程序应在一个合理的时间应用于现有系统,此时间由业主/经营者决定。

4.3 职责

符合本文件是业主/经营者的职责。

5 报警系统模型

5.1 报警系统

报警系统用于向操作员,即监视和操作过程的人员,传达异常过程状况或设备故障并支持响应。有效的报警系统均是经过良好的设计、实施、操作和维护的。报警管理是确保有效报警系统的一系列实践和过程。

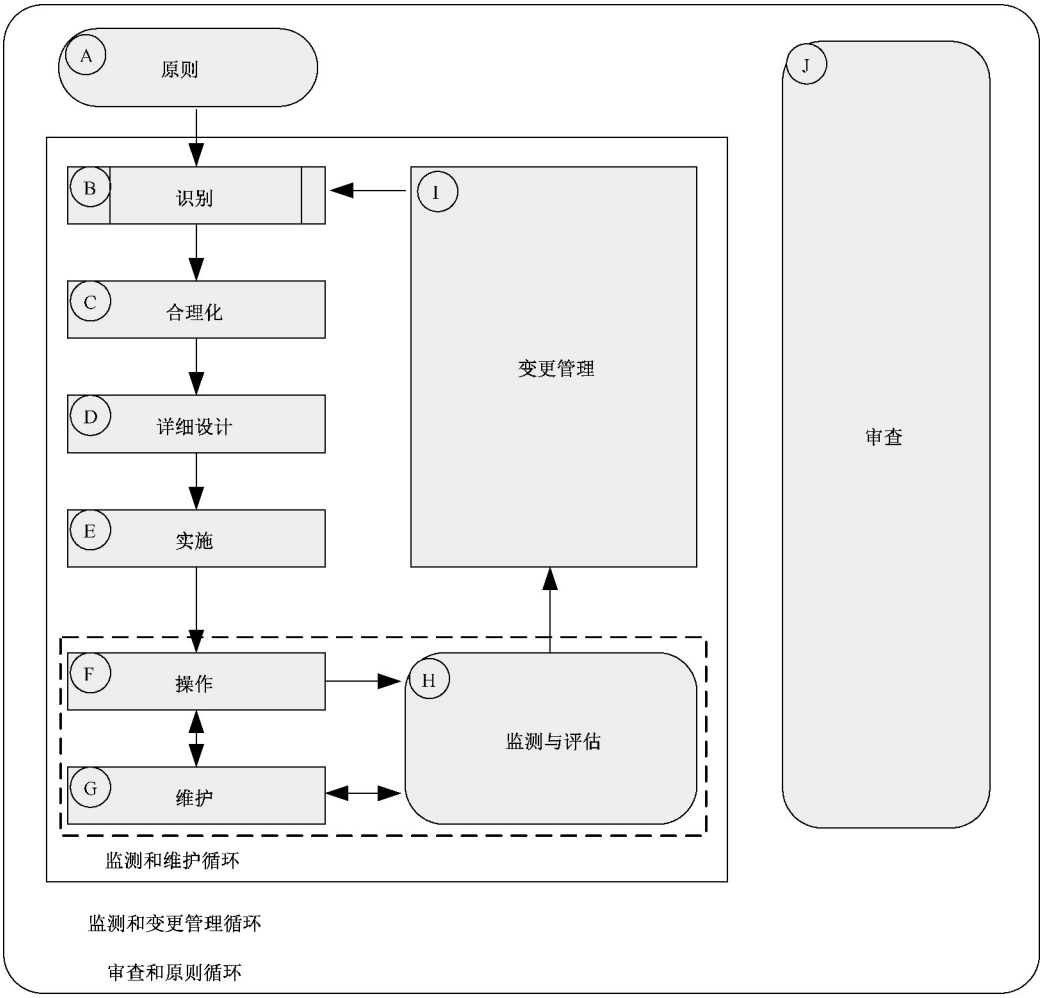
报警管理的基础部分是报警的定义,即通过一种有声和/或可视的方式向操作员指示需要响应的设备故障、过程偏差或其他异常状况,该定义的一个关键要素是对报警的响应。本文件描述的报警管理流程对该定义进行了进一步阐释。

5.2 报警管理生命周期

5.2.1 报警管理生命周期模型

图 2 阐明了本文件中所规定的报警管理生命周期各阶段之间的关系。报警管理生命周期包含报警系统从最初的概念直至停用之间的规范、设计、实施、运行、监测、维护、变更活动。

此生命周期模型在确定实施报警管理系统的要求和责任方面极其有用。此生命周期模型适用于新报警系统的安装或现有系统的管理。



注 1：按照 5.2.2.3 的规定，用于阶段 B 的方框代表确定于本文件之外的流程。

注 2：按照 5.2.2.11 的规定，独立阶段 J 代表一个连接到所有其他阶段的流程。

注 3：按照 5.2.3 的规定，阶段 A、阶段 H 和阶段 J 的圆角矩形代表生命周期的切入点。

注 4：按照 5.2.5 的规定，虚线表示生命周期中的循环。

图 2　报警管理生命周期

5.2.2　报警管理生命周期各阶段

5.2.2.1　综述

图 2 所示的报警管理生命周期各阶段的简要描述如下。字母标签是文本中使用的标识符。本文件的第 6 章～第 18 章阐述了各阶段的要求和建议。

5.2.2.2　报警原则(A)

在设计新的报警系统或修改现有系统之前，必须制定基本规划。通常，第一步是制定报警原则，确定报警系统的目标以及实现这些目标的流程。对于新系统，报警原则是报警系统要求规范(ASRS)文件的内容基础。

报警原则从基本定义着手，并将其扩展到操作性定义。报警优先级标准以及报警分类、性能标准、性能限制和报告要求的定义均基于报警系统的目标和原则。报警原则还包含在人机界面中显示报警的

方案，包括优先级的使用，这应与人机界面的总体设计一致。报警原则确定了报警管理生命周期各阶段所使用的流程，例如变更管理流程的门槛以及变更的具体要求。报警原则用于确保报警管理在报警系统全生命周期内的一致性。

报警原则阶段包括报警系统要求规范的编制，该规范可由工厂依据自身情况特别设定，提供具体的限制或选项，并且可以作为新系统选型或改造现有控制系统的参考依据。该规范通常比报警原则更具体，可为系统设计提供具体指导。

5.2.2.3 识别(B)

识别阶段是一个信息收集点，收集各种决定是否需要设置报警的方法提出的潜在报警。这些方法在本文件之外定义，所以本文件中将识别阶段表示为一个预定义流程。这些方法可以是正式的，例如工艺危险分析、安全要求规范、事故调查建议、良好的生产实践、环境许可、P&ID 编制或操作程序评审。工艺变更和运行测试同样可能要求新增报警或修改已有报警。报警系统性能的日常监测也可以识别出一些报警变更需求。在此阶段，新增报警或修改已有报警的需求被识别出，以进行后续的合理化论证。

5.2.2.4 合理化(C)

合理化阶段将已识别出的新增报警或修改已有报警的需求与报警原则中的原则相协调。这些步骤可以在一个流程中完成或分步完成。合理化的输出成果是报警说明书，包括所有可用于完成报警设计的高级报警技术。

合理化是应用报警要求生成支持性文档的过程，例如报警设定值的依据、可能的危害后果以及操作员可以采取的纠正措施。

合理化包括根据报警原则中所定义之方法对报警进行优先级排序。报警的优先级通常取决于可能的危害后果以及容许的响应时间。

合理化还包括对报警的分类，将报警分配给一个或多个类别以指明相应要求(例如：设计、测试、培训或报告要求)。危害后果的类型或其他标准可用于将报警分为报警原则中所定义的不同类别。

通常，合理化结果记录于主报警数据库(例如：经批准的文件或文档)，在报警系统全生命周期留存。

5.2.2.5 详细设计(D)

在设计阶段，根据合理化阶段确定的要求细化并设计各报警属性。设计包括三个方面：基本报警设计、人机界面设计和高级报警技术设计。

基本报警设计遵循基于不同报警类型和具体控制系统的指南。

人机界面设计包括报警显示和警报，包括报警优先级的指示。

高级报警技术是指在基本报警设计和人机界面设计之上用于提高报警系统有效性的附加功能。这些技术包括基于状态的报警。

5.2.2.6 实施(E)

报警或报警系统的安装及投运均在实施阶段完成。新建报警或报警系统的实施包括系统的物理和逻辑安装以及功能验证。

由于操作员是报警系统的重要组成部分，所以操作员培训是实施过程中的一项重要活动。对新建报警的测试通常是一个实施要求。

用于培训、测试和调试的文档可能会随报警原则中所定义的不同分类而变化。

5.2.2.7 操作(F)

在运行阶段,报警或报警系统处于运行状态,并执行其预期功能。这个阶段包括报警原则和各报警的目的的巩固培训。

5.2.2.8 维护(G)

在维护阶段,报警或报警系统无法运行,处于测试或修理状态。定期维护(例如:仪器的测试)是必要的,以确保报警系统按设计运行。

5.2.2.9 监测与评估(H)

在监测与评估阶段,报警系统和各报警的总体性能将根据报警原则中规定的性能目标进行持续监测。对运行阶段的数据进行监测和评估,可能会触发维护工作或识别出对报警系统或操作程序的变更需求。对维护阶段的数据进行监测和评估可以指示维护效率。报警系统的整体性能也根据报警原则中所规定的目标进行监测和评估。如果没有监测,报警系统的性能可能会降级。

5.2.2.10 变更管理(I)

针对报警系统的修改在变更管理阶段提出并批准。变更流程应遵循报警管理生命周期各阶段,从识别到实施的相关要求。

5.2.2.11 审查(J)

在审查阶段,定期进行审查,以维持报警系统和报警管理程序的完整性。对系统性能的审查可以发现常规监测中不明显的缺陷。对报警原则的执行情况进行审查,以识别系统改进需求,例如,修改报警原则。审查还能识别是否需要增加组织规则以遵循报警原则。

5.2.3 报警生命周期切入点

5.2.3.1 综述

根据所选择的方法,报警管理生命周期包括三个切入点:

a) 报警原则;

b) 监测和评估;以及

c) 审查。

上述切入点由图2中的圆角矩形表示。作为切入点,生命周期的这些阶段仅为管理报警系统的初始步。完整的报警管理系统应具备生命周期所有阶段。

5.2.3.2 报警原则切入点(A)

第一个可能的起始点是制定一个报警原则,该原则可以确定报警系统的目标,并可以作为报警系统要求规范的基础。这是新建报警系统的生命周期切入点。

5.2.3.3 监测和评估切入点(H)

第二个可能的起始点是开始监测现有报警系统并评估其性能。通过维护或变更管理来识别和解决问题报警。在制定报警原则之前,监测数据可以用于基准评估。

5.2.3.4 审查切入点(J)

第三个可能的起始点是利用一套书面记载的实践对报警管理的所有方面进行初始审查或基准测试,例如,在本文件中列出的那些实践。初始审查结果可以用于制定报警原则。

5.2.4 阶段间的同步和包含关系

生命周期图(图 2)是以顺序的方式描绘各阶段。事实上,生命周期包括多个同步阶段,有些阶段包含了其他阶段的活动。

监视和评估阶段(H)与运行和维护阶段是同时的。

变更管理阶段(I)表示变更流程的开始。通过此流程,生命周期的所有适用阶段都得到了授权和完成。

审查阶段(J)是一个可以在生命周期的任何时候发生的总体活动,包括对其他阶段活动的审查。

5.2.5 报警管理生命周期循环

5.2.5.1 综述

除了报警管理生命周期的各个阶段,生命周期还包括三个循环。

在一个周期内,每个循环执行一项功能。

5.2.5.2 监测和维护循环

运行-监测和评估-维护循环是识别需要维护的问题报警的常规监测。问题报警在修复后将恢复运行状态。

5.2.5.3 监测和变更管理循环

当常规监测显示报警设计与报警原则不兼容时,将触发运行-监测与评估-变更管理循环。报警设计可能需要进行修改,或者需要应用高级报警技术。启动变更管理流程以及重复生命周期的各个阶段的同时,报警系统可以继续运行。

5.2.5.4 审查和原则循环

审查-原则循环是生命周期本身以及报警系统持续改进的过程。审查流程识别出生命周期中需要强化的流程。

5.2.6 报警管理生命周期各阶段输入和输出

报警管理生命周期各阶段是联系在一起的,因为一个阶段的输出通常是另一个阶段的输入。在生命周期图(图 2)中,这些联系并未完全得到表示,关于生命周期各阶段的输入和输出之间的关系的更多信息,如表 1 所示。

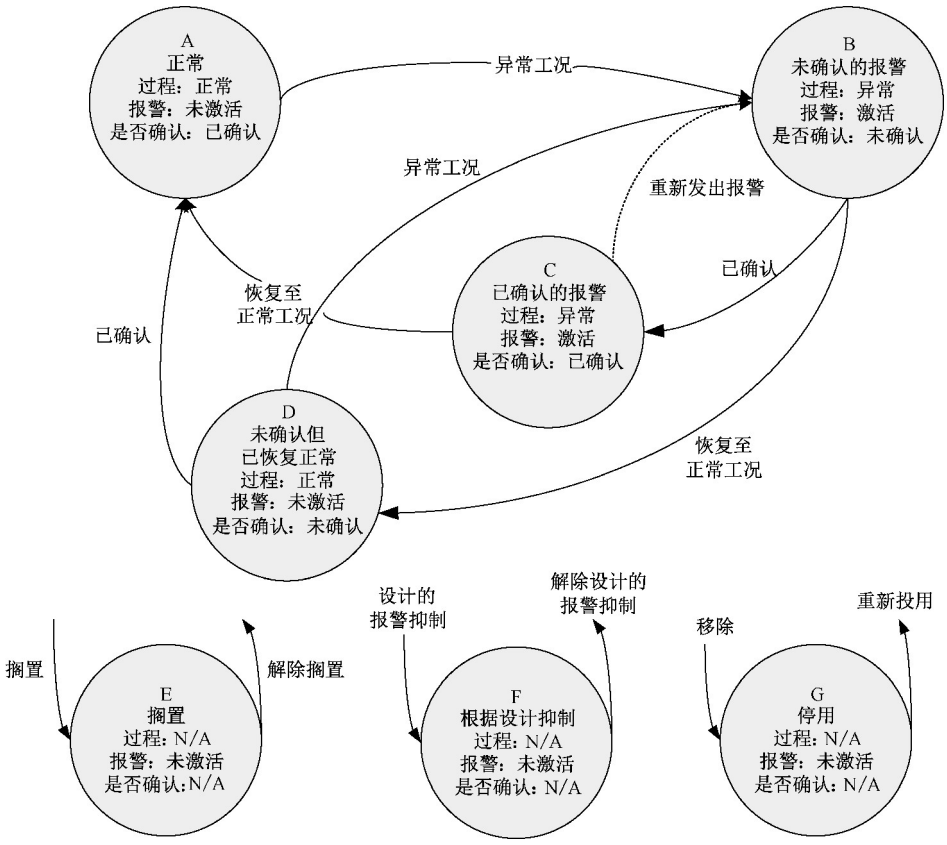
表 1　报警管理生命周期阶段输入和输出

报警管理生命周期阶段		活动	条目编号	输入	输出
阶段	类目				
A	原则	编制报警管理以及 ASRS 的目标、指导方针和工作流程	第 6 章,第 7 章	目标和标准	报警原则和 ASRS
B	识别	确定潜在报警	第 8 章	PHA 报告、SRS、P&ID、操作程序等	潜在报警列表
C	合理化	合理化、分类、确定优先级和文件编制	第 9 章	报警原则和潜在报警列表	主报警数据库和报警设计要求。
D	详细设计	基本报警设计、HMI 设计和高级报警设计	第 10 章,第 11 章,第 12 章	主报警数据库和报警设计要求	已完成的报警设计
E	实施	安装报警、实施测试和巩固培训	第 13 章	已完成的报警设计和主报警数据库	运行报警和报警响应程序
F	运行	操作员对报警做出响应和复习训练	第 14 章	运行报警和报警响应程序	报警数据
G	维护	维护、维修和更换以及定期测试	第 15 章	报警监测报告和报警原则	报警数据
H	监测和评估	监测报警数据和报告性能	第 16 章	报警数据和报警原则	报警监测报告和变更提议
I	变更管理	授权增加、修改和删除报警的流程	第 17 章	报警原则和提议的变更	已授权的报警变更
J	审查	报警管理程序的定期审查	第 18 章	标准、报警原则和审查协议	改进建议

5.3　报警状态

5.3.1　报警状态转换图

图 3 所示的报警状态转换图表示出了典型报警的各种状态和各种状态间的转换。虽然存在例外，该图形描述了大多数报警的情况，可为制定报警系统原则和 HMI 功能提供有用的参考。



注 1：状态 E、F 和 G 可以连接到图中的任何报警状态。

注 2：虚线表示一个很少实施的选项。

图 3　报警状态转换图

5.3.2　报警状态

5.3.2.1　综述

图 3 中的圆圈表示报警的状态，字母标签是一个标识符，第二行是状态名称，通常采用缩略词，第三行描述了过程状态，第四行和第五行分别列出了报警状态及其确认状态。图底部显示了可能的报警抑制状态。

5.3.2.2　正常状态(A)

正常(NORM)报警状态被定义为过程运行在正常范围的状态，报警未被激活，并且过去的报警已经得到确认。

5.3.2.3　未确认状态(B)

未确认(UNACK)的报警状态是由异常工况引起报警的初始状态。在这个状态下，报警还未被确认。以前已确认的报警可以被设计为重新报警，使其恢复到这个状态。

5.3.2.4　已确认状态(C)

已确认(ACKED)的报警状态是报警处于激活状态，操作员已经确认了该报警。

5.3.2.5 未确认但已恢复正常的状态(D)

在未确认但已恢复正常(RTNUN)的报警状态时,过程处于正常范围内,报警在操作员确认报警状态之前变为未激活状态。

5.3.2.6 搁置状态(E)

当报警处于搁置(SHLVD)状态时,报警通过受控的方法被暂时抑制,无法发出报警。处于搁置状态的报警受操作员的控制。搁置功能可以自动解除报警的搁置状态。

5.3.2.7 依据设计抑制的状态(F)

在依据设计抑制的(DSUPR)报警状态下,报警根据运行状态或装置状态被抑制,无法发出报警。设计的抑制状态下的报警处于逻辑控制之中,它决定了报警的相关性。

5.3.2.8 停用状态(G)

在停用(OOSRV)状态下,报警通过手动抑制被移除(例如:通过控制系统的移除功能移除某个报警),无法发出报警,通常是为了实施维护作业。在停用状态下的报警处于维护控制。

5.3.2.9 报警状态

不同报警状态下的告警状况总结如表 2 所示。

表 2 报警状态

标识符	助记符	状态名称	过程状态	报警状态	通告状态	确认状态
A	NORM	正常的报警状态	正常	未激活	未通告	已确认
B	UNACK	未确认的报警状态	异常	激活	已通告	未确认
C	ACKED	已确认的报警状态	异常	激活	已通告	已确认
D	RTNUN	未确认但已恢复正常的报警状态	正常	未激活	已通告	未确认
E	SHLVD	搁置状态	正常或异常	激活或未激活	抑制	不适用
F	DSUPR	依据设计抑制的报警状态	正常或异常	激活或未激活	抑制	不适用
G	OOSRV	停用的报警状态	正常或异常	激活或未激活	抑制	不适用

5.3.3 报警状态转化路径

5.3.3.1 综述

图 3 中的箭头表示不同状态之间的转换。为简单起见,该图并未阐明报警死区和延迟或解除延迟的影响。

5.3.3.2 从正常状态向已确认状态转换(A －＞ B)

当过程超出正常范围即超过报警设定值并且保持这个状态足够长以触发报警时,则发生此转换。

5.3.3.3 从未确认状态向已确认状态转换(B －＞ C)

操作员在过程恢复至正常状态前确认某个被激活的报警,则发生此转换。

5.3.3.4 从已确认状态向未确认状态转换(C －＞ B)

此转换很少使用,当报警处于报警状态时,此转换会使单一报警周期性地产生重复的报警信号。

5.3.3.5 从已确认状态向正常状态转换(C －＞ A)

此转换是报警的正常顺序。报警从已确认状态向正常状态转换。

5.3.3.6 从未确认状态向未确认但已恢复正常的状态转换(B －＞ D)

当过程在操作员确认报警之前恢复至正常状态,则发生此转换。

5.3.3.7 从未确认但已恢复正常的状态向正常状态转换(D －＞ A)

报警恢复到正常状态并变为未激活状态后发生此转换,可以要求操作员确认或自动确认。

5.3.3.8 转换至搁置状态(任何状态－＞ E)

当操作员搁置某个报警以避免激活报警的混乱显示时,该转换发生。搁置是一个手动操作。

5.3.3.9 从搁置状态向正常或未确认状态转换(E －＞ A or B)

当报警被手动或自动地解除搁置,该转换发生。如果报警处于未激活状态,则转换至正常状态。如果报警处于激活状态,则转换至未确认状态。

5.3.3.10 转换至依据设计抑制(任何状态－＞ F)

依据报警设计,当过程条件或状态被用于抑制报警时,则该转换发生。所设计的抑制通常是自动操作。

5.3.3.11 从依据设计抑制的状态向正常或未确认状态转换(F －＞ A or B)

在适当的时候,当过程条件或状态被用于解除报警抑制时,则该转换发生。所设计的解除报警抑制通常是自动操作。如果报警处于非激活状态,则转换至正常状态。如果报警处于激活状态,则转换至未确认状态。

5.3.3.12 转换至停用状态(任何状态－＞ G)

为实施维护或者其他原因,可移除报警。移除通常是手动操作。

5.3.3.13 从停用状态转换至正常或未确认状态(G －＞ A 或 B)

当可用时,已停用报警可重新投用。重新投用通常是手动操作。如果报警处于未激活状态,则转换至正常状态。如果报警处于激活状态,则转换至未确认状态。

5.4 报警响应时间轴

5.4.1 综述

图 4 表示某个过程测量从正常状态增加至异常状态,以及基于操作员是否采取纠正措施的两种可能情景。图 3 中的一些报警状态可以映射到图 4 所示的时间轴,以阐明与时间相关的术语的定义。

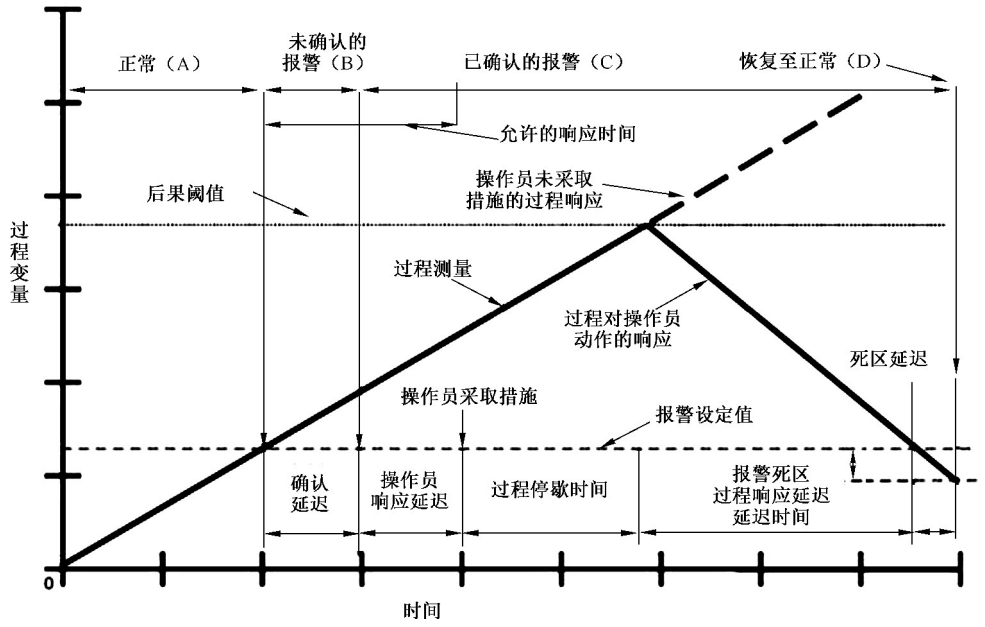


图 4　报警响应时间轴

5.4.2　正常状态(A)

正常状态被定义为过程运行在正常的规范中的状态，报警是未激活的，且所有之前的报警都已被确认。

5.4.3　未确认状态(B)

当测量超过报警设定值时即进入未确认的报警状态。影响警报发出的几个因素如下所示：

a)　测量精度；

b)　采样间隔；以及

c)　报警延迟。

操作员并不总能立即确认报警。

5.4.4　已确认状态(C)和响应

在延迟一段时间后，当操作员确认报警状况时，即达到已确认的报警状态。在此状态下报警是激活的。影响操作员响应时间的几个因素如下所示：

a)　系统处理速度；

b)　人机界面设计和清晰度；

c)　操作员认知和培训；

d)　操作员工作量；

e)　判定操作员应采取的动作的复杂性；以及

f)　操作员动作的复杂性。

报警的实际响应时间是指报警发出开始到操作员采取纠正措施结束的整个时间段。它包括报警检测、情况诊断、操作员响应动作确定以及响应执行。响应时间的上限是允许的响应时间，一旦超过该时间点，即使采取了措施，后果依然会发生。

5.4.5 恢复至正常状态(D)

恢复至正常状态是指在允许的响应时间内操作员采取了正确的措施。影响恢复至正常状态的时间的几个因素如下所示：

a) 操作员响应延迟；
b) 纠正措施的执行程度；
c) 响应纠正措施的过程停歇时间；
d) 响应纠正措施的过程响应时间；
e) 过程测量的精确度；
f) 报警设定值的死区；以及
g) 报警系统的运行速度。

5.4.6 后果阈值

当操作员未采取措施时，或采取的措施不正确或不充分时，或在允许的响应时间内未完成操作时出现的后果。当达到后果阈值时，后果开始出现。

5.5 操作员与过程交互的反馈模型

5.5.1 综述

操作员与过程交互的模型如图5所示。由于对干扰或故障的响应，过程或系统会发生一些变化，如果变化明显偏离了过程的参考状态或目标，操作人员则采取措施将过程恢复至参考状态，并在恢复后继续监视测量。为了使动作发生，需要发生如下三个阶段的活动：

a) 检测到与期望的正常操作的偏差；
b) 诊断工况并确定纠正措施；以及
c) 实施纠正措施以补偿扰动。

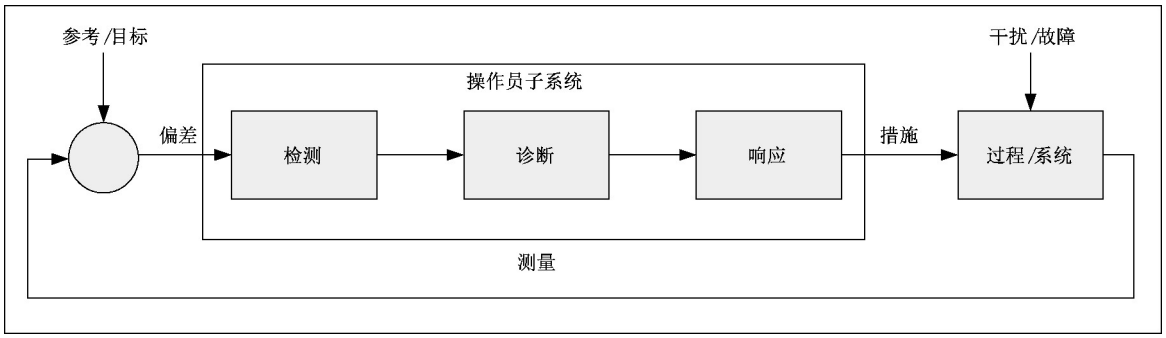


图5 操作员与过程交互的反馈模型

5.5.2 检测

操作员通过报警注意到过程与期望状态的偏差。报警系统的设计和操作员界面促进了偏差的检测。

5.5.3 诊断

操作员运用相关知识和技能来解释信息、诊断工况并确定需要采取的纠正措施以应对偏差。

5.5.4 响应

操作员执行纠正措施以应对偏差。

5.5.5 绩效影响因素

操作员执行子系统功能的能力受各种因素的影响，包括工作负荷、短期或工作记忆限制、疲劳、培训和激励。

6 报警原则

6.1 目的

报警原则是报警管理生命周期的一个单独阶段。报警原则作为一个框架，为报警管理生命周期各阶段建立标准、定义、原则和职责。这是通过具体的项目来实现的，包括报警识别、合理化、监测、变更管理以及跟踪审核。报警原则文档可促进：

a) 报警系统的一致性；

b) 与风险管理目的和目标的一致性；

c) 与良好工程实践的一致性；以及

d) 有效支撑操作员响应的报警系统的设计和管理。

6.2 报警原则内容

6.2.1 综述

6.2 提供了报警原则应包括的最基本内容及推荐包括的内容。由于过程工业使用的设备种类繁多，报警原则的详细内容在不同行业和不同地域可能不同。报警原则要求的和推荐的内容如表 3 所示。

表 3 要求的和推荐的报警原则内容

报警原则内容	要求/推荐	条款编号
报警系统的目的	要求	6.2.2
定义	要求	6.2.3
参考	要求	6.2.4
报警管理的角色和职责	要求	6.2.5
报警设计原则	要求	6.2.6
合理化	要求	6.2.7
报警分类定义	要求	6.2.8
高级别管理报警(或现场同等级别)	推荐	6.2.9
HMI 设计原则	要求	6.2.10
优先级确定方法	要求	6.2.11
报警设定值确定	推荐	6.2.12

表 3　要求的和推荐的报警原则内容（续）

报警原则内容	要求/推荐	条款编号
报警系统性能监测	要求	6.2.13
报警系统维护	要求	6.2.14
报警系统测试	要求	6.2.15
经核准的增强级和高级报警技术	推荐	6.2.16
报警文档	要求	6.2.17
实施指南	要求	6.2.18
变更管理	要求	6.2.19
培训	要求	6.2.20
报警历史保存	要求	6.2.21
相关现场程序	推荐	6.2.22
特殊的报警设计考虑	推荐	6.2.23
报警系统审查	要求	6.2.24

对于为新装置设计的报警系统，报警原则应作为项目计划和开发的一部分，在报警合理化之前充分地进行定义和批准。

对于正在进行改造的没有报警原则的现有报警系统，报警原则应是改造工作的第一阶段。

报警原则所需的内容可以存在于其他现场程序。这些程序应在报警原则中进行参考引用。

6.2.2　报警系统的目的

过程装置报警系统的目的和目标需要进行定义。定义清晰的目的和目标可以为设计和改进活动的参与者提供指引。此定义可以促进有效的报警系统的实施和维护。

6.2.3　定义

在设计和改进报警系统过程中所出现的术语应进行定义，以确保所有的参与者理解一致。

6.2.4　参考

报警原则中应包含报警管理适用的参考。参考可以是公司内部文件（例如：变更管理）或者外部的出版资料。

6.2.5　报警管理的角色和职责

报警原则中应确定报警管理生命周期系列活动的职责，具体方面包括如下：

a）　报警系统、原则和相关文件的所有者；

b）　负责管理报警系统并进行定期维护的角色；

c）　负责技术支持以解决报警系统的各种问题的角色；

d）　负责确保报警原则中所列要求均被遵循的角色。

6.2.6 报警设计原则

报警的定义以及符合和不符合定义的实例应记录于报警原则中。报警设计的选择准则和原则应与报警定义保持一致。

准则和原则应当说明：

a) 报警系统在识别不安全的或次优的操作方法、警告故障并提醒操作员对过程进行可操作的修改中的作用；

b) 用于报警识别的方法；

c) 装置将用到的报警状态(例如：正常状态、已确认状态、搁置状态等)。

6.2.7 合理化

为了使报警系统功能最大化，操作员应只接收需要操作员响应的报警，这一点尤为重要。通过报警合理化确保报警需要得到响应。报警原则的此部分应当列出评估报警的准则和合理化应获得的信息。

此部分应为合理化团队应具备的知识和经验提供指导，应包括：

a) 操作；

b) 工艺；

c) 控制系统；以及

d) 报警原则。

6.2.8 报警分类定义

报警分类用于设置管理报警的通用要求。一个报警可以属于多个分类。此部分应包括报警分类的定义。

此部分还应包括以下类别要求：

a) 报警文档；

b) 操作员培训和培训文档；

c) 与报警相关的操作程序；

d) 报警维护；

e) 报警测试；

f) 报警监测和评估；

g) 报警变更管理；

h) 报警历史记录；

i) 报警审查；

j) 报警优先级；以及

k) HMI 设计。

6.2.9 高级别管理报警

高级别管理报警(HMA)分类是指与其他分类相比需要更严格管理和文档记录的报警分类。由于准则可能因工艺、行业或地点产生差异，因此如果应用 HMA，报警原则应定义将报警指定为 HMA 的标准。进行高级别管理的报警分类应当基于以下一个或多个条件：

a) 对于保护人员生命的过程安全关键的报警(例如：安全报警)；

b) 针对人员安全和保护的报警；

c) 针对环境保护的报警；
d) 针对现行良好生产实践的报警；
e) 针对商业损失的报警；
f) 针对产品质量的报警；
g) 工艺许可方要求的报警；以及
h) 公司政策要求的报警。

如果应用 HMA 分类，报警原则的这个部分应记录针对这些报警分类的要求。

6.2.10 HMI 设计原则

确定报警呈现给操作员的方法、格式和编码（例如：颜色、符号和字母数字），制定显示报警和发出报警的原则，使其在整个工厂保持一致。

此部分应包括的具体内容如下：

a) 向操作员传递报警的机制（例如：面板、BPCS 控制屏等）；
b) 将用于装置中 HMI 上的各种报警状态（例如：正常、已确认、搁置等）的指示建议；
c) 将采用的显示类型（例如：报警汇总、首出报警等）；
d) HMI 中将设置的功能，包括搁置功能和抑制功能。

6.2.11 确定优先级的方法

一致的优先级有助于操作员在高报警率期间决定响应次序。此部分应包括的具体内容如下：

a) 确定报警优先级的依据（例如：后果的严重程度、响应时间等）；
b) 报警配置标准（例如：报警总数和优先级分配）；
c) 划分优先级的影响。

6.2.12 确定报警设定值

此部分应提供用于确定报警设定值的方法指南。

6.2.13 报警系统性能监测

各种度量标准被用于监测报警系统性能，和目标性能水平相比。

此部分提供性能评估依据，以决定是否需要改进。

此部分应涵盖的具体内容如下：

a) 监测和评估目标；
b) 监测度量标准和目标值；
c) 关于报警系统性能审查频率的指南；以及
d) 关于提高性能的方法的指南。

6.2.14 报警系统维护

此部分明确了维护报警系统所需要的活动。

此部分应涵盖的具体内容如下：

a) 报警维修记录保留；
b) 关于停用报警的要求；以及
c) 临时报警使用原则。

6.2.15 报警系统测试

此部分确定为确保报警系统在全生命周期的一致性和充分测试的相关程序。测试的适用性、准则、方法和频率应按报警分类进行充分的书面记录。

6.2.16 经核准的增强级和高级报警技术

经核准的增强级和高级报警技术及其使用条件或准则应当进行鉴别。鉴别经核准的增强级和高级报警技术可以支持针对这些技术的人员培训。

并不是所有的工厂都会使用增强级和高级报警技术(参见第 12 章)。如果一个工厂确实使用了增强级和高级报警技术,报警原则的这部分应被用来确认采用的技术和相关职责及工作流程。

6.2.17 报警文档

报警原则中应当提出适当的文档要求,可包括以下几个方面:

a) 合理化信息(例如:主报警数据库);

b) 定期报警性能报告;

c) 高级报警管理技术规范;以及

d) 关于依据设计抑制的规范。

根据不同报警分类的要求还可提出其他文档需求。

适当的文档可确保高级技术实施的一致性,规范操作员在所有操作模式中的操作行为。

6.2.18 实施指南

确定初始培训、调试和报警系统检测的基本方法,从而促进整个工厂或公司的一致性,确保报警系统的有效部署。

6.2.19 变更管理

此部分确定了变更类别和适用程序。变更管理程序应当被书面记录。变更类别可包括:

a) 报警的暂时性变更(例如:停用);

b) 主报警数据库、报警属性或增强级和高级报警技术的永久性变更。

永久性变更应遵循变更管理程序,以确保在设计、实施、运行或维护过程中的变更得到适当地评估、获得授权方的批准并进行书面记录。通常,此过程包括针对每个变更的评估的书面记录、系统修改记录和授权。

6.2.20 培训

此部分详细说明了如何对工厂人员进行关于报警系统的使用、管理和设计的培训。此部分还详细说明了对培训文档的要求。

应在报警原则或其他同等文档中涵盖的针对每个报警分类培训的具体方面包括以下:

a) 报警系统相关的需要培训的工作岗位或人员;

b) 培训内容大纲;以及

c) 要求进行培训的时间点。

6.2.21 报警历史保存

此部分确定了应当保存的报警历史的哪些方面(例如:发出报警、确认、恢复至正常状态以及操作员

动作)以及留存周期(例如:不利事件、违反安全操作限制)。在某些行业和地区,监管机构或地方法规可能要求保存这些信息。

6.2.22 相关现场程序

为避免报警原则和其他现场程序间出现不一致,报警原则应当引用相关程序。下列文档可能与报警原则相关:

a) 标准操作程序;
b) 操作员培训策略和指南;
c) 安全、健康和环境程序;
d) 维护程序;
e) 报警处理策略和准则;
f) 应用程序编程指南;
g) 调试或合格认定流程及程序;
h) 变更管理程序;以及
i) 基于特定现场,与报警原则相关的其他现场程序。

6.2.23 特殊的报警设计考虑

原则文件应当确定包涵特殊情况的报警的设计规则和方法,其中一致性尤为重要(例如:旁路报警和冗余传感器报警)。报警分类可能是此类特殊设计考虑的源头。

6.2.24 报警系统审查

原则文件应当明确对定期报警管理审查的要求。这些要求包括:

a) 根据报警分类确定的审查频率;
b) 审查主题;以及
c) 操作员访谈流程。

6.2.25 报警原则开发和维护

应用报警原则的人员应参与报警原则的制定。参与团队应具备并理解现场相关过程的设计、操作和维护的详细知识。

具体的专业领域包括:

a) 过程操作;
b) 过程检测仪表;
c) 控制系统;
d) 过程技术;
e) 机械/可靠性工程;
f) 安全、健康和环境;
g) 过程安全;
h) 人为因素;
i) 报警管理;以及
j) 变更管理流程。

7 报警系统要求规范

7.1 目的

报警系统要求规范(ASRS)也被称为报警功能要求规范,是报警原则生命周期阶段的一部分。第7章为报警系统要求规范的开发和应用提供了指南。ASRS记录了控制系统的预期报警功能。

ASRS通常是控制系统整体系统要求规范的一个子集。

报警系统要求规范通常特定于某个现场、单个控制系统或一组相似的控制系统。ASRS在与报警原则保持一致的同时,比报警原则包含了更详细的关于报警系统功能的要求,包括详细的用户要求并考虑了相关现场基础设施的要求。这些要求用于帮助评估系统,指导详细的系统设计并在实施过程中作为报警系统功能测试的主要依据。区分ASRS和单个报警活动(发生在系统生命周期的更晚时候)至关重要。ASRS确定了在合理化、设计、实施、可视化和记录单个报警以及在分析报警记录时要提供的报警功能。

ASRS通常在规划一个新控制系统的早期制定,在实施阶段进行更新,以确保与所选系统的目标能力保持一致,因此,它与推动系统设计、系统测试和培训活动等方面具有相关性。在系统实施之后,ASRS通常不再进行更新。报警系统功能的变更可能在系统的生命周期内发生。这些变更可以通过变更管理进行管理并记录。

7.2 推荐规范

新控制系统的规划和对现有控制系统的报警功能的重大修改应包括ASRS,ASRS包含以下部分或全部规范:

a) 报警属性;
b) 报警HMI;
c) 报警通信协议;
d) 报警记录日志;
e) 报警记录分析;以及
f) 其他有助于报警生命周期活动的功能。

新的控制系统项目也可能不需要ASRS(例如:复制现有系统)。省略ASRS的决定及支撑该决定合理性的说明应当被书面记录。

7.3 制定

报警系统仅是控制系统中的一个功能系统,为了控制系统的整体性能可能需要报警系统要求做出妥协。报警原则包含可用于制定某些报警系统要求规范的指南。ASRS应包括以下内容:

a) 可用的报警优先级;
b) 可视警报功能,例如,颜色和符号;
c) 有声警报功能;
d) 报警汇总显示功能;
e) 报警搁置功能;
f) 报警抑制功能;
g) 报警组态功能,例如,死区、报警延迟和解除延迟;
h) 报警日志功能;

i) 报警监测和评估功能；
j) 报警系统审查功能；以及
k) 高级报警功能。

一些报警要求可存在于其他文档，例如：IEC 61511 中的 SIS 安全要求规范。

7.4 系统评估

在控制系统选择过程中，应根据需求对报警系统功能性进行评估。从非常有限到非常先进，不同控制系统的报警系统功能性不同。报警系统要求规范提供了一个具体标准的列表，可用于不同系统的比较评估。

7.5 定制

如果标准的商业产品未能满足规范中某些重要的系统要求，则有必要开发定制解决方案或者重新考虑该规范。

报警系统要求规范有利于较早识别定制解决方案需求，还可触发相关成本/利润分析。

7.6 报警系统要求测试

在生命周期的运行阶段之前，每个报警系统要求均应进行测试。

8 识别

8.1 目的

识别是报警管理生命周期中的一个单独阶段。识别是可以用来确定潜在报警需求或变更报警需求的不同方法的一个通用术语。识别阶段是报警生命周期中确定建议的报警或报警变更的输入点。识别出的报警是合理化阶段的一个输入。

8.2 报警识别方法

本文件不规定或要求任何特定的报警识别方法。报警可以通过各种良好的工程实践或法规要求进行识别。可将某些识别方法结合在一起用于确定潜在报警。在适当的地方，报警识别可在报警合理化过程中进行。

一些通用的报警识别方法如下：

a) 安全层分配；
b) 工艺危险分析(PHA)；
c) 危害与可操作性分析(HAZOP)；
d) 保护层分析(LOPA)；
e) 事故调查；
f) 环保环境许可；
g) 故障模式和影响分析(FMEA)；
h) 现行良好生产实践(cGMP)；
i) 质量评审；
j) P&ID 评审；
k) 操作程序评审；以及

l) 成套设备制造商的建议。

8.3 识别培训

使用任何方法进行报警识别的人员都应针对报警原则和报警评估标准进行培训。

9 合理化

9.1 目的

合理化是报警管理生命周期中的一个单独阶段。在合理化过程中,现有或潜在的报警将被系统地与报警原则中设定的报警标准进行比较。

如果所提出的报警符合标准,则对报警设定值、后果和操作员动作进行记录,并根据报警原则对报警进行优先级排序和分类。

合理化生成了报警生命周期设计阶段需要的详细设计信息。

对于每种适用装置状态下按报警原则进行合理化的每个报警,合理化应至少确定并记录如下几个方面:

a) 报警类型;
b) 优先级;
c) 分类;
d) 报警设定值或逻辑条件(例如:异常);
e) 操作员动作;
f) 不响应或不正确动作的后果;
g) 可能的原因;以及
h) 如必要,对高级报警技术的需求。

9.2 合理化文档

9.2.1 合理化文档要求

针对每个报警的合理化文档应包括(必须)如下几个方面:

a) 报警类型;
b) 优先级;
c) 分类;
d) 报警设定值或逻辑条件(例如:异常);
e) 操作员动作;
f) 不响应或不正确动作的后果。

9.2.2 合理化文档推荐规范

针对每个报警的合理化文档还应包括(推荐)以下几个方面:

a) 允许的最长响应时间;
b) 可能的原因;
c) 识别方法;以及
d) 如必要,对高级报警技术的需求。

9.3 报警证实

9.3.1 报警证实流程

每一个需要合理化的报警都与报警原则中的标准进行比较，以证实该报警的必要性。

来自报警定义的标准包括：

a) 报警是针对操作员的；

b) 报警指示某个过程偏差、异常工况或设备故障；以及

c) 报警需要及时响应。

9.3.2 证实方法

报警证实流程应：

a) 利用团队协作的方法；

b) 高度信赖操作员输入；以及

c) 关注被提示的操作员动作。

9.3.3 单个报警证实

所有需要合理化的报警都需进行系统的审查。这通常是通过工程制图、数据库或 HMI 显示来完成的。应在报警原则中确定每个合理化报警需获得的信息，但通常包括：

a) 验证提出的报警是否符合报警原则中规定的报警标准；

b) 操作员可以采取的响应措施；

c) 如果未采取措施或措施失败将发生的后果；

d) 警报发出和具体后果发生之间所需要的时间。

对于那些操作员只需简单地将信息传递给相应的人员或组织去采取行动的报警(例如：仪表诊断报警)，应进行审查以确定是否存在替代的方法来传送信息而不用操作员或报警系统负担。

9.3.4 对报警系统的影响

报警证实应确保：

a) 该报警不会成为一个妨碍；以及

b) 该报警不是对某个要求相同操作员动作的报警的复制。

高级报警技术(例如：基于状态的报警或基于逻辑的报警)可以进行详细说明以防止对报警系统产生负面影响。

9.4 报警设定值确定

可使用报警原则中规定的报警设定值确定指南。

有效的报警设定值确定方法应综合考虑允许的响应时间(参见图 5)、操作员动作的复杂性、过程操作的知识和历史以及其他因素。

9.5 优先级确定

应用报警原则中定义的优先级分配方法给合理化报警分配优先级。高效的优先级分配结果通常是高优先级比低优先级选用频率低。大多数报警应被分配为最低报警优先级(最不重要的)，极少数被分配为最高报警优先级(最重要的)，并在两者之间进行一致的转换。优先级分配结果应与后果和允许的

响应时间保持一致，使得最低优先级的报警具有最不严重的后果和最长的允许响应时间，最高优先级的报警具有最严重的后果（例如：火灾和可燃气体报警）和最短的允许响应时间。第16章提供了优先级分配标准。

优先级确定可能包括对报警分类的考虑（例如：HMA分类）或识别方法的考虑（例如：LOPA），以设置报警优先级。

9.6 移除

不符合报警原则中规定的报警标准的现有报警及其应被移除的依据（即其不符合的标准）应被记录。

这些报警应按照MOC程序进一步进行审核，以从系统中移除这些报警。

9.7 分类

分类是在报警生命周期的合理化阶段完成一项工作。

根据报警原则中的定义，报警应被分配给一个或多个分类。

同一分类中的报警无需有相同的优先级。报警分类可在报警证实和优先级确定之前、过程中或之后进行。

9.8 审查

在完成全部要求的报警的初步证实、优先级确定和分类后，应对结果进行审查，以确保在整个过程中一致地应用了相关标准。审查结果应与报警原则中预先设定的报警的数量和优先级的目标进行比较。

9.9 文档使用

合理化过程应被书面记录以成为确保报警系统完整性的基础资料。合理化文档（例如：一个主报警数据库）阐释了每个报警和报警原则之间的联系，并且可以用于多个目的，包括：

a) 输入到报警生命周期中的详细设计阶段；
b) 作为变更管理的一部分进行应用；
c) 操作员培训以及供操作员审查；
d) 控制系统报警设置的定期审查和核对；以及
e) 对报警监测及效果数据的评估。

10 详细设计：基本报警设计

10.1 目的

基本报警设计是生命周期中详细设计阶段的一部分。第10章阐释了在特定的控制系统中实施合理化过程所定义的报警的基本要求。同时，第10章针对与触发报警相关的设计考虑提出了解决方案。而所有与报警展示相关的设计考虑均被纳入第11章。

10.2 报警状态的使用

10.2.1 报警状态触发

系统中每个报警的触发诱因均需进行记录。在控制系统内不同诱因所能触发的报警状态的改变如

图 1 所示，其中包括如下几个方面：

a) 现场设备(例如：传感器和执行单元)；

b) 控制和安全系统；以及

c) HMI。

10.2.2 报警状态和其他逻辑功能

关于报警状态信息和其他逻辑功能的使用，应提供明确的设计指南(例如：联锁功能)。如果报警设定值在操作员通知之外还将用于其他目的(例如：作为联锁设定值)，则文档、培训和变更管理均将受到影响。此外，修改报警属性的影响以及依据设计抑制的使用也需要明确进行识别、记录和可能地限制(例如：所需的额外确认或更高的访问级别)。上述信息应明确记录于报警原则中的报警设计原则下面。

10.2.3 报警抑制和其他逻辑功能

报警抑制功能不能旁路其他逻辑功能(例如：联锁功能)。

10.3 报警类型

合理化时定义的每个报警均需分配一个报警类型。定义报警类型旨在为操作员提供不同报警的视觉区别。常见的报警类型如下：

a) 绝对值报警；

b) 偏差报警；

c) 变化率报警；

d) 状态偏差报警；

e) 计算报警；

f) 配方驱动的报警；

g) 位模式报警；

h) 控制器输出报警；

i) 系统诊断报警；

j) 仪表诊断报警；

k) 可调节报警；

l) 自适应报警；

m) 重新发出报警；

n) 统计报警；

o) 首出报警；

p) 坏值报警。

不同控制系统中包含的可用的报警类型不同。可能需要创建一些自定义报警类型作为一个项目工程范围的一部分。

报警类型应根据工程判断进行谨慎选择。如果应用不当，某些类型在异常情况下常成为滋扰报警的来源，如变化率报警、偏差报警、坏值报警以及控制器输出报警。

10.4 报警属性

10.4.1 综述

在基本设计过程中，应为合理化时确定的每个报警设置默认报警属性，设置应基于工程评价。

根据所实施的特定报警类型，诸如设定值和死区等属性可能不同。定义适当的报警属性有助于将运行过程中产生的滋扰报警的数量减至最小。10.4.2～10.4.6 提供了针对特定报警属性设计的推荐规范。报警属性应包括：

a) 报警设定值或逻辑条件；
b) 报警类型；
c) 报警优先级；
d) 报警组；
e) 报警延迟或报警解除延迟；
f) 死区；以及
g) 报警信息。

10.4.2 报警描述

所有报警都应有一个信息文本，以标签描述或报警描述或两者均有的形式提供。推荐使用结构化的形式和一致性术语。

10.4.3 报警设定值

报警设定值应根据主报警数据库中记录的信息进行配置。

10.4.4 报警优先级

报警优先级应根据主报警数据库中记录的信息进行分配。

10.4.5 报警死区

10.4.5.1 综述

报警死区是控制系统中的一个报警属性，它要求过程变量以某个确定的增量或百分比，越过报警设定值进入正常操作范围内。死区通常是根据过程变量的正常操作范围、测量噪声和过程变量的类型进行设置。使用死区可以非常有效地排除滋扰报警。

10.4.5.2 报警死区要求

控制系统应具备实施死区功能的能力。

10.4.5.3 关于报警死区的建议

报警原则中应记录设置死区的工程基础。设置死区时应进行工程评价，以实现最小化滋扰报警的同时确保过程警戒和装置及人员安全。

过大的死区可能因其锁存器功能导致陈旧报警，例如一个测量范围较大的仪表（如，0 到 100 的流量）。死区设置值应进行书面记录，然后在试车过程中和获得充分运行经验后进行审查。

10.4.6 报警延迟和解除延迟

10.4.6.1 综述

报警延迟和解除延迟属性（即去抖动定时器）可以用于排除滋扰报警。报警延迟用于避免信号临时超过其设定值时发出不必要的报警，即在信号处于报警状态并持续特定的时长后方才触发报警。报警解除延迟用于减少抖动报警，即在过程条件恢复正常后将报警指示继续保持一段时间。

10.4.6.2 报警延迟和解除延迟要求

控制系统应提供实现报警延迟和解除延迟功能的能力。

10.4.6.3 关于报警延迟和解除延迟的建议

设置报警延迟和解除延迟时应进行工程评价,以实现最小化滋扰报警的同时确保过程警戒和装置及人员安全。

延迟时间应考虑所有操作模式下的过程响应时间,以及是否采用过滤来减少信号噪声。报警延迟时间仅当谨慎评估潜在控制系统的运行效果后才可应用。延迟时间设置应在试车过程中和获得充分运行经验后进行审查。

10.5 报警属性的编程更改

某些现场需根据一些条件(诸如批次配方、产品类型或品号)修改报警属性。报警属性通常可通过下面列出的一种或多种方式进行更改:

a) 操作员界面(例如:运行过程中的手动更改);
b) 工程界面(例如:变更管理下的设计变更);
c) 控制逻辑(例如:顺序和阶段);
d) 高级报警技术;
e) 控制系统之外的系统[例如:制造执行系统(MES)、企业资源规划(ERP)系统]。

报警原则应详细说明该功能的使用和限制。针对每个报警,用户都应确认并明确记录系统的哪些程序在操作过程中可对报警属性进行修改,以及哪些修改需受控于变更管理程序。第12章包含了用于修改报警属性的高级报警技术的相关内容。

10.6 审查基本报警设计

一个典型的控制系统为用户提供针对单个过程变量实现多种不同报警类型的能力。为了最小化操作员的报警负载,应参照主报警数据库对基本报警设计结果进行审查,以确保仅保留必要的报警。

11 详细设计:报警系统的人机界面设计

11.1 目的

报警系统的HMI设计是详细设计生命周期阶段的一部分。第11章概述了为操作员和其他HMI用户提供的报警指示及相关功能。报警的指示和显示仅是HMI设计的一个组成部分,有助于有效的操作员-过程交互(参见图5)。关于控制系统的综合HMI设计的指南不属于本文件范围。

11.2 人机界面功能

11.2.1 综述

报警的HMI设计应与报警原则和整体HMI设计原则保持一致。HMI设计应考虑控制系统的能力。

11.2.2 人机界面信息要求

HMI应清晰地指示:

a) 激活的报警；
b) 报警状态；
c) 报警优先级；以及
d) 报警类型。

11.2.3 人机界面功能要求

人机界面应为操作员提供以下功能：
a) 静音有声报警指示（未确认报警）；
b) 确认报警；
c) 通过报警原则允许的访问受控方法停用报警；
d) 仅通过访问受控方法修改报警属性；
e) 启动报警搁置功能；
f) 显示报警信息；
g) 将报警分配给操作员站。

11.2.4 人机界面显示要求

人机界面应提供以下或同等性能：
a) 报警汇总显示；
b) 在过程显示上进行报警指示；
c) 在标签细节显示上进行报警指示；
d) 搁置报警汇总显示；以及
e) 停用报警汇总显示。

11.2.5 报警记录要求

报警记录是一组记录报警状态变化的信息。
报警记录应具有以下报警记录属性：
a) 报警的标识名；
b) 报警的标签说明或报警描述；
c) 报警状态；
d) 报警优先级；
e) 报警类型；以及
f) 报警状态发生变化的时间和日期。

11.2.6 关于报警记录的建议

报警记录应有以下要素：
a) 记录报警记录时的过程值，
b) 报警设定值；
c) 所在过程区域；
d) 所属报警组；以及
e) 报警信息。

11.3 报警状态指示

11.3.1 综述

报警状态转换图(参见图3)定义了报警的状态。

11.3.2 要求的报警状态指示

应利用视觉指示、听觉指示或两者结合的方式独特地区分以下报警状态：

a) 正常；
b) 未确认报警；
c) 已确认报警；
d) 未确认但已恢复正常的报警；
e) 搁置报警；
f) 依据设计抑制的报警；以及
g) 停用报警。

11.3.3 推荐的报警状态指示

11.3.3.1 综述

以下所推荐的报警状态指示是常见的行业惯例。

11.3.3.2 正常状态指示

正常状态不应使用声音指示。正常状态的视觉指示应与未报警的指示相同。

11.3.3.3 未确认的报警状态指示

未确认的报警状态应同时采用有声指示和视觉指示。有声指示需通过操作员执行消音动作或确认动作进行静音。视觉指示应通过使用颜色和符号(例如：形状或文本)与正常状态指示进行明确的区分。未确认报警的视觉指示应包括一个闪烁元素。在某些环境中，有声指示不是一个有效的未确认报警指示。

11.3.3.4 已确认的报警状态指示

已确认的报警状态不应使用有声指示。已确认的报警状态的视觉指示应使用符号(例如：形状或文本)与正常状态指示进行明显区分，其颜色应与未确认的报警指示一致。闪烁元素不应用于已确认的报警的视觉指示。

11.3.3.5 未确认但已恢复正常的状态指示

未确认但已恢复正常的状态不应使用有声指示。未确认但已恢复正常的状态的视觉指示可以与正常状态相同，或者可以通过闪烁元素指示未确认状态。

11.3.3.6 搁置报警状态指示

搁置报警状态应在人机界面上进行视觉指示。搁置报警的视觉指示不应包含闪烁元素，搁置报警状态指示应是独特的。有声指示不应被用于确认搁置报警。

11.3.3.7 依据设计抑制的报警状态指示

人机界面中应直观地显示依据设计抑制的报警状态。依据设计抑制的报警的视觉指示不应包含闪烁元素。依据设计抑制的报警状态指示应与未确认状态指示和已确认状态指示不同。有声指示不应用于识别依据设计抑制的报警。

11.3.3.8 停用报警状态指示

停用的报警状态应在人机界面中直观地进行显示。停用报警的视觉指示不应包含闪烁元素。停用报警状态指示应与未确认状态指示和已确认状态指示不同。有声指示不应用于识别停用报警。

11.3.3.9 报警状态指示汇总

针对典型报警所推荐的有声和视觉报警指示汇总如表4所示。

表4 推荐的报警状态指示

报警状态	声音指示	视觉指示		
		颜色	符号	闪烁情况
正常	否	否	否	否
未确认报警	是	是	是	是
已确认报警	否	是	是	否
未确认但已恢复正常的报警	否	组合		可选择的
搁置报警	否	组合		否
依据设计抑制的报警	否	组合		否
停用报警	否	组合		否
“是”表示应使用该指示类型来指示该报警状态。 “否”表示不应使用该指示类型来指示该报警状态。				

11.3.4 有声报警状态指示

根据报警原则，用于未确认报警的有声报警指示也可用于指示优先级、过程区域或报警组。

在未确认报警的有声指示无效的环境中（例如：外界噪声等级较高的环境），未确认报警指示应采用始终在操作员视野内的清晰的视觉指示（例如：一个灯光或一系列灯光）。

11.4 报警优先级指示

11.4.1 综述

报警原则规定了人机界面中使用的一组报警优先级，以帮助操作员选择报警响应动作的先后顺序。

11.4.2 报警优先级指示要求

应使用视觉指示、有声指示或两者的独特组合来区分报警系统内的报警优先级。

11.4.3 颜色报警优先级指示要求

每个报警优先级都应使用一个单独的颜色指示，在操作环境中除外（在操作环境中不实用）。报警

优先级颜色应预留,不得用于人机界面的其他元素。

11.4.4 推荐的报警优先级指示

11.4.4.1 综述

以下推荐的报警优先级指示是常见的行业惯例。

11.4.4.2 符号报警优先级指示

一个独特的符号(例如:形状或文字)应被用来指示每一个报警优先级以加强颜色编码。

11.4.4.3 有声报警优先级指示

每个报警优先级应使用一个有声指示。在有声指示未作为优先级指示的环境中,视觉优先级指示应被选用。

11.5 报警信息指示

11.5.1 综述

报警信息提供了标识名、状态和优先级指示之外的进一步的报警说明。它也可能包括部分操作员操作或对报警响应程序的引用。

11.5.2 推荐的报警信息指示

11.5.2.1 综述

以下推荐的报警信息指示是常见的行业惯例:

a) 视觉报警信息指示;以及

b) 有声报警消息指示。

11.5.2.2 视觉报警信息指示

应为每个报警生成一个视觉报警信息并显示在报警汇总中。通常,视觉报警信息不直接显示在过程显示中。

11.5.2.3 有声报警信息指示

语音合成器可用于有声报警信息。有声报警信息应是结构化的、简短的。有声报警信息可由操作员通过消音动作或者确认动作进行静音。视觉指示应与有声报警信息结合使用。

11.6 报警显示

11.6.1 综述

在人机界面内,作为报警系统的一部分有几种类型的显示是有效的。这些包括以下几点:

a) 报警汇总显示;

b) 报警汇总状态显示;

c) 报警日志显示;

d) 过程显示;

e) 标签内容显示;

f) 系统诊断报警显示；
g) 搁置报警显示；
h) 停用报警显示；
i) 依据设计抑制的报警显示。

11.6.2 报警汇总显示

11.6.2.1 报警汇总显示要求

报警汇总显示至少需要一个。报警汇总提供了报警系统内处于激活状态的报警的列表。报警汇总显示有几个要求的和推荐的功能。

11.6.2.2 信息要求

报警汇总显示应只列出报警信息。报警汇总显示应提供每个报警的以下信息：
a) 报警标识名；
b) 报警的标签说明或报警描述；
c) 报警状态(包括确认状态)；
d) 报警优先级；
e) 报警激活时间/日期；
f) 报警类型。

11.6.2.3 信息建议

报警汇总显示应提供每个报警的以下信息：
a) 过程值；
b) 报警设定值；
c) 所属过程区域；
d) 所属报警组；
e) 报警信息。

11.6.2.4 推荐的附加信息

除了每个报警的信息外，报警汇总应显示：
a) 汇总表中的报警数量；
b) 汇总表中未确认报警的数量。

11.6.2.5 功能要求

报警汇总显示应提供以下功能：
a) 按时间顺序排序报警；
b) 按优先等级排序报警；
c) 针对每个报警的单个确认；以及
d) 视觉报警的确认。

11.6.2.6 功能建议

报警汇总显示应提供以下功能：

a) 导航到适当的过程显示的链接；
b) 按报警时间筛选报警；
c) 按优先级筛选报警；
d) 按报警类型筛选报警；
e) 按报警组筛选报警；
f) 按过程区域筛选报警；
g) 按标识名筛选报警；
h) 针对筛选器的时间限制；以及
i) 按标识名排序报警。

在报警汇总显示中使用筛选器的地方，显示时应清晰标明正在使用筛选器。时间限制功能可以在时间周期结束时移除筛选器。

11.6.3 报警汇总状态

11.6.3.1 综述

建议使用报警汇总状态显示。报警汇总状态显示为每个过程区域提供了按优先级分类的活动报警数量的指示。

11.6.3.2 信息建议

报警汇总状态显示应为每个过程区域或其他分组提供以下信息：
a) 每个报警优先级下的报警数量；
b) 每个优先级下未确认的报警数量；
c) 关于某个优先级下所有报警是否均被确认的指示。

11.6.3.3 功能建议

报警汇总状态显示应提供一个导航到适当的过程显示的链接。

11.6.4 报警日志显示

11.6.4.1 综述

应提供一个报警日志显示。报警日志显示提供了对报警日志的访问途径，它包含每个报警状态变化的报警记录(例如：确认、恢复正常等)。

11.6.4.2 信息建议

报警日志显示应为报警记录提供以下信息：
a) 报警的标识名；
b) 报警的标签说明或报警描述；
c) 报警状态(包括确认状态)；
d) 报警优先级；
e) 报警的日期和时间；
f) 确认报警的日期和时间；
g) 恢复正常的日期与时间；以及
h) 报警类型。

11.6.4.3 功能建议

报警日志显示应提供以下功能：

a) 按标识名筛选报警；
b) 按报警时间筛选报警；
c) 按优先级筛选报警；
d) 按报警类型筛选报警；
e) 按报警组筛选报警；以及
f) 按过程区域筛选报警。

11.6.5 过程显示

过程显示为报警提供了一个过程环境。过程显示应提供以下信息：

a) 标识名(通过文本或其他访问方法)；
b) 报警状态，包括确认状态；
c) 报警优先级；
d) 报警抑制状态；以及
e) 报警类型。

11.6.6 标签内容显示

标签内容显示为报警的标签提供详细信息，标签内容显示应提供以下信息：

a) 报警状态(包括确认状态)；
b) 报警优先级；
c) 报警组；
d) 报警类型；
e) 报警设定值；
f) 报警抑制状态；以及
g) 过程变量的当前值或状态。

11.6.7 其他显示要素

其他可以用来指示报警状态的显示要素。

11.7 报警搁置

11.7.1 综述

操作人员暂时搁置报警是用于防止滋扰报警妨碍报警系统有效性的一个功能。搁置包括确保保持报警系统完整性的功能。

11.7.2 报警搁置功能要求

报警搁置功能应提供以下：

a) 搁置报警的能力；
b) 显示搁置报警列表或等同列表的功能，以指示处于搁置状态的所有报警；
c) 搁置的时间限制；

d) 用于搁置单个报警的访问控制；
e) 解除报警的搁置状态的能力；以及
f) 关于每个搁置报警的记录。

时间限制是在时间段到期时解除报警的搁置状态的功能。

11.7.3 关于报警搁置的功能建议

报警搁置功能应被设计为能防止处于激活状态的报警自动解除搁置时发生报警泛滥。

a) 手动解除搁置的报警应转换到已确认的报警状态。
b) 自动解除搁置的报警应转换到未确认的报警状态。

11.7.4 搁置报警显示

11.7.4.1 综述

具有搁置功能的报警系统的搁置报警显示(或等效列表功能)有几个要求的和推荐的功能。

11.7.4.2 信息要求

搁置报警显示应提供以下信息：

a) 报警的标识名；
b) 报警的标签说明或报警描述；
c) 报警类型；
d) 报警状态(即激活或未激活)；
e) 报警优先级；以及
f) 搁置的剩余时间或报警被搁置的时间和日期。

11.7.4.3 功能要求

搁置报警显示应提供以下功能：

a) 按时间顺序或搁置的剩余时间排序报警；
b) 按优先级排序报警；
c) 通过标签排序报警；以及
d) 解除单个报警搁置。

11.7.4.4 功能建议

搁置报警显示应提供以下功能：

a) 按优先级筛选报警；
b) 按报警状态筛选报警；
c) 按过程区域筛选报警；
d) 操作员输入报警被搁置的原因；
e) 按组解除报警搁置；
f) 导航到过程显示的链接；以及
g) 导航到标签详细内容显示的链接。

11.8 停用报警

11.8.1 综述

通过将报警停用来抑制报警是移除报警以进行维护的常规做法。有几种与停用报警有关的要求和推荐的人机界面功能。

11.8.2 停用报警功能要求

停用报警功能应提供以下内容：

a) 单个地停用各个报警的方法；
b) 单个地恢复各个报警的方法；
c) 显示停用报警或等同列表的功能，以指示处于停用状态的所有报警；
d) 如果允许，通过访问控制停用报警；以及
e) 关于每个被停用的报警的记录。

11.8.3 停用报警显示

11.8.3.1 停用报警显示要求

报警系统应具有停用报警显示或等效列表功能。停用报警显示有多个要求的和推荐的功能。

11.8.3.2 信息要求

停用报警显示应提供以下信息：

a) 报警的标识名；
b) 报警的标签说明或报警描述；
c) 报警类型；
d) 解除抑制的报警状态(即激活或未激活)；
e) 报警优先级；以及
f) 停用报警的时间和日期。

11.8.3.3 功能要求

停用报警显示应提供以下功能：

a) 按照抑制时间顺序排序报警；
b) 按优先级排序报警；
c) 按报警状态排序报警(即激活或未激活)；
d) 按过程区域排列报警；以及
e) 单个地将报警恢复使用。

11.8.3.4 功能建议

停用报警显示应提供操作员输入报警被抑制的原因的功能。

11.9 依据设计抑制的报警

11.9.1 综述

设计的报警抑制是抑制由于预期的或实际的操作条件而不需要的报警的常规做法。

11.9.2 设计抑制功能要求

设计抑制功能应提供以下内容：

a) 显示依据设计抑制的报警列表或等效列表的功能，以指示依据设计抑制的所有报警；以及

b) 关于依据设计抑制的每个报警的记录。

11.9.3 设计抑制功能建议

设计抑制功能应被设计为能防止处于激活状态的报警自动解除抑制时发生报警泛滥。自动解除抑制的报警应转换到未确认的报警状态。

11.9.4 依据设计抑制的报警的显示

11.9.4.1 综述

应为报警系统提供依据设计抑制的报警显示或等效列表功能。依据设计抑制的报警显示有多个要求的和推荐的功能。

11.9.4.2 信息要求

依据设计抑制的报警显示应提供以下信息：

a) 报警的标识名；

b) 报警的标签说明或报警描述；

c) 报警类型；

d) 解除抑制的报警状态(即，报警状态为激活的或未被激活的)；

e) 报警优先级；以及

f) 报警被抑制的时间和日期。

11.9.4.3 信息建议

依据设计抑制的报警显示应提供抑制方法的指示(例如：设计的抑制)。

11.9.4.4 功能要求

依据设计抑制的报警显示应提供以下功能：

a) 按抑制时间顺序排序报警；

b) 按优先级排序报警；

c) 按报警状态排序报警；以及

d) 按过程区域排序报警。

11.10 警报器集成

11.10.1 综述

报警系统可以包括单独的警报装置。11.10 描述了关于将独立警报器集成到报警系统的建议。

11.10.2 警报器集成建议

警报器应被集成到报警系统以提供以下功能：

a) 将报警状态信息通信到报警日志；

b) 防止控制系统中的冗余报警；

c) 避免需要在控制系统中冗余确认。

11.10.3 警报器显示集成建议

警报器应被集成到报警系统，以使得报警器的报警布局遵循一致的方法论。

11.11 安全报警人机界面

11.11.1 综述

根据标准或规范要求，一些安全报警需设置独立的人机界面。安全报警的识别方法不在本文件范围内。

11.11.2 独立的安全报警人机界面

以下安全报警可能要求设置独立于 BPCS 的人机界面：

a) 安全相关报警，根据关注点（例如：风险降低因子）；以及

b) （指示危险故障）指示危险故障的 SIS 系统诊断报警，根据关注点（例如：操作员响应、通信故障）。

注：更多指南请参见 GB/T 21109（所有部分）。

12 详细设计：增强级和高级报警方法

12.1 目的

增强级和高级报警是详细设计生命周期阶段的一部分。在控制系统中通常使用的报警管理技术之外，第 12 章提供了关于附加的报警管理技术的指南和注意事项。它们通常在基本的报警系统设计基础上提供了额外的功能，特别有助于指导操作员在异常过程条件下的操作。

增强级和高级报警方法是用于修改报警属性的附加的逻辑、编程或建模层，这些方法包括动态报警、基于状态的报警（即基于模式的报警）和自适应报警。大多数依据设计抑制方法都包含在高级报警技术中。

除了高级报警技术之外，报警系统的增强也为操作员提供了增强的信息。这类信息通常被认为是避免或减轻可能导致事故的运行问题所必需的。

基本报警设计方法可能不足以减少报警泛滥或减轻其影响，因此可能需要增强级和高级技术。这些方法可以减少或消除报警泛滥。

12.2 增强级和高级报警基础

12.2.1 综述

如果基本报警设计没有实现报警原则中规定的性能目标，那么经常使用增强级和高级报警方法来实现这些目标。报警原则或报警系统要求规范应包括可接受的增强级和高级报警方法的列表。

12.2.2 工作量、人力需求和复杂性

增强级和高级报警技术外加的复杂性需要额外的资源来设计、实施和维护。变更管理流程应包括审查变更对增强级和高级报警技术的影响。

报警系统复杂性增加带来的成本应与报警系统性能的提高进行比较。

在批准前和设计时,应考虑增强级和高级报警技术失效场景的风险分析。

12.3 信息链接

通过链接到主报警数据库中的信息(例如:操作员动作或后果)可以增强报警系统。信息也可以从其他来源链接,包括:操作程序、操作员日志、维护历史记录或设计文档。这些链接应易于管理和维护。

12.4 基于逻辑的报警

12.4.1 综述

基于逻辑的报警是使用布尔逻辑或决策树来确定对报警系统所做的修改。

12.4.2 报警属性修改

对于一些增强级和高级报警技术来说,修改某些报警属性(例如:报警设定值或优先级)的功能是必需的。

12.4.3 外部授权系统

外部授权系统捕获来自控制系统的报警和过程数据,并使用这些信息来确定设施运行情况以及相应的报警属性修改。

12.4.4 逻辑报警抑制和属性修改

逻辑报警抑制技术使用来自某些报警的报警状态条件来修改其他报警的报警属性(例如:先出报警)。

12.4.5 基于状态的报警

基于状态的报警是一种高级报警技术,可根据设备或过程的已定义操作状态来修改报警设定值、优先级或抑制状态。状态通常是通过以下信息决定:

a) 逻辑变量的状态;

b) 定义的过程变量达到特定的限度;

c) 考虑许多变量和指标的逻辑;以及

d) 操作员选择。

状态确定和报警修改可以通过手动、半自动(例如:手动和自动化的某种组合)或者全自动模式进行。状态应清晰地展示给操作员。

12.5 基于模型的报警

基于模型的报警可以用在需要更复杂的报警系统的地方,复杂的过程参数可以产生基于多个数据点的结果,或者可以由模型得出对工厂状态的估计。

在未进行详尽的分析前,基于模型的报警系统不应被用来替代基本报警系统。

12.6 附加报警注意事项

12.6.1 综述

一些附加的增强功能增加了报警系统价值,这些增强功能通常可以在基本报警系统中获得。

12.6.2 非控制室注意事项

如果希望操作员在完成非控制室任务的同时对报警进行响应，则可以考虑采用远程报警显示和确认方式。可能需要建立相关程序以向后备操作员发出报警。当使用远程报警系统时，报警原则应包括这些系统。

使用远程报警通知的做法应包括定期测试信息以提高可靠性。应考虑建立一个程序来确保对报警的响应。

12.6.3 远程报警系统

可能存在几种情况，最需要了解异常情况并对其采取行动的人不是控制室中的操作员，这些情况可以受益于远程报警系统（例如：寻呼、电子邮件等）。

消息传送的可靠性是远程报警系统中的一个重要问题，应予以考虑。可能也需要提供远程确认。

12.6.4 辅助报警系统

辅助报警系统（例如：报警响应专家系统）可以替代控制系统的报警通知系统或利用现有的图形环境来提供通用界面。或者，在现有的报警系统之外，使用辅助系统来提供附加的或替代的报警信息。

应特别注意确保附加信息提供价值，系统的设计应确保报警的可用性和可靠性是可接受的。

当使用辅助报警系统时，该辅助报警系统应符合本文件的所有要求。

12.6.5 批处理过程注意事项

12.6.5.1 综述

过程条件、状态和阶段可用于修改批处理过程中的报警，这通常以基于状态的报警进行实施。

12.6.5.2 连续可变的报警阈值

批处理过程报警通常仅适用于过程的特定步骤，或者与变化的控制回路设定值或时变过程数据趋势相关联。除非特别注意，批处理过程特别容易产生滋扰报警。高级报警技术可以提供一个结构，以解决这些与批处理相关的报警问题。

12.6.5.3 相对时间和绝对时间

通常，数据和报警记录在计算机系统中按日历时间记载。对于批处理的信息，相对时间（即从批次或过程步骤开始的时间）具有更强的相关性。高级报警功能能够利用日历时间和电子记录指示批处理步骤或阶段开始的时间，以及进行计算并以相对时间显示报警。

12.6.5.4 包含批号和其他识别标志

某些现场可能会设置将识别编码与报警相关联的功能。能够根据选定的标识对记录进行排序，有利于生成正式批次记录以及比较不同批次的记录。选取和附加这种识别标志的方法应被验证并可靠。

12.7 培训、测试和审查系统

报警原则应规定确保高级报警技术持续运行的相关步骤，包括培训、测试和审查。培训、测试和审查程序应包括增强级和高级报警技术。

12.8 报警属性强制

为了保持设计的报警属性设置(例如:报警设定值和报警优先级)处于核准值,应将合理化值与控制系统中的实际设置值进行定期比较。强制,即报警属性的自动验证和恢复,是一种增强级报警技术,用来执行与监视、评估和审查相关的功能。强制可以按照计划进行,也可以根据要求进行,并应区分于基于状态的报警或报警搁置方法造成的修改。

13 实施

13.1 目的

实施是报警管理生命周期的一个单独阶段,是从设计到运行的过渡。第13章涵盖了实施或修改一个报警或报警系统的一般要求。

13.2 实施计划

项目或变更的范围将决定所需工作的范围。

实施计划应包括以下考虑因素:

a) 操作中断;

b) 能胜任的资源的可用性;

c) 功能测试或验证;

d) 文件验证;

e) 操作员培训。

13.3 实施培训

13.3.1 综述

新报警和现有报警修改的培训要求由报警的分类和报警原则中对于不同分类的具体要求决定。

13.3.2 实施培训

在操作员承担响应新的或修改的报警的责任之前,操作员应接受针对所有新的或修改的报警响应所实施的培训。

13.3.3 实施培训要求

培训应包括:

a) 报警的合理化信息(例如:后果、报警原因、纠正措施等);以及

b) 报警的有声和视觉指示。

13.3.4 高度管理的报警的培训文件要求

新的或修改的高度管理报警的培训文件应包括:

a) 接受培训的人员;

b) 培训方法;以及

c) 培训日期。

13.3.5 关于培训文件的建议

培训的文件应包括：

a) 接受培训的人员；

b) 培训方法；

c) 培训日期。

13.3.6 新的或修改的报警系统的实施培训要求

操作员应接受所有新的或修改的报警系统的培训。

13.3.7 关于新的或修改的报警系统实施培训的建议

修改的报警系统的培训要求应适合变更性质，新报警系统的培训要求应包括：

a) 报警的声音和视觉指示；

b) 报警优先级的区分；

c) 报警人机界面功能的使用(例如：报警汇总排序和过滤)；

d) 搁置和抑制方法；以及

e) 移除报警的方法。

13.4 实施测试和验证

13.4.1 综述

新报警和现有报警修改的实施测试要求由报警分类和报警原则中对于不同分类的具体要求决定。

13.4.2 高度管理的报警的实施测试要求

报警原则应确定高度管理报警在投入运行之前的测试要求，测试应被记录在案，包括：

a) 报警设定值或逻辑条件；

b) 报警优先级；

c) 报警的有声和视觉指示；

d) 规定的报警的任何其他功能要求；

e) 进行测试的人员；

f) 测试方法和验收标准；

g) 测试结果和测试失败或不符合项的解决方案；

h) 测试日期；以及

i) 报警投用的日期。

13.4.3 关于新的或修改的报警实施测试的建议

报警应在实施过程中进行测试，测试应包括验证：

a) 报警设定值或逻辑条件；

b) 报警优先级；

c) 报警的声音和视觉指示；以及

d) 规定的报警的任何其他功能要求。

13.4.4 新的或修改的报警系统的实施测试要求

报警系统应在实施过程中进行测试，以确保符合报警原则和报警系统要求规范的相应条款。修改后的报警系统的测试应适合现场变更管理程序确定的变更性质。新报警系统的测试应包括：

a) 每个报警优先级的声音和视觉指示；
b) 人机界面功能(例如：报警汇总中的报警信息或同等功能)；
c) 移除报警和恢复报警的方法；
d) 搁置报警的方法；
e) 抑制报警的方法；
f) 任何附加的增强级或高级报警技术功能；
g) 报警过滤、排序、链接报警到过程显示的方法。

13.5 实施文件

13.5.1 综述

关于报警系统实施的文件要求和建议。

13.5.2 文件要求

应当提供以下文件：

a) 记录的合理化信息；
b) 足够的信息来执行报警测试；
c) 报警响应程序；以及
d) 任何设计的抑制或增强级报警文档。

报警系统实施完成后，合理化信息应按现场变更管理程序进行更新。

13.5.3 关于实施文件的建议

报告方法、文件格式和结构应符合项目文件程序和业主的文件要求。

测试方法和文件应适合于现场变更管理程序或报警原则确定的变更性质。

测试新的和修改的报警时使用的信息可能包括以下内容：

a) 报警的标识名；
b) 报警的标签说明或报警描述；
c) 报警类型；
d) 优先级；
e) 报警设定值或逻辑条件；
f) 操作员操作；
g) 不采取行动的后果；
h) 测试和变更的日期；
i) 测试方法和验收标准；
j) 测试结果和测试失败或不符合项的解决方案。

14 运行

14.1 目的

运行是报警管理生命周期的一个单独阶段。第14章涵盖了保持在运行状态及恢复到运行状态的报警的要求。运行状态是指当报警能够向操作员指示异常情况的时候。还描述了在运行状态下使用工具进行报警处理。运行是实施阶段或从维修阶段恢复之后的生命周期阶段。

14.2 报警响应程序

14.2.1 报警响应程序要求

报警响应程序应易于操作员获取。

14.2.2 关于报警响应程序的建议

应使用操作人员认为最易理解的报警文档格式。在报警合理化过程中所记录的报警信息也应易于获取。

除报警原则另有规定外,报警响应程序应包括:

a) 报警标识名;
b) 报警的标签说明或报警描述;
c) 报警类型;
d) 报警设定值;
e) 潜在原因;
f) 不采取行动的后果;
g) 操作员动作;
h) 允许响应时间;以及
i) 报警分类。

14.3 报警搁置

14.3.1 报警搁置要求

应根据报警原则中对于不同报警分类的具体要求允许报警搁置。

14.3.2 搁置高度管理的报警

如果使用了高度管理的报警类别,搁置高度管理的报警时应遵循报警原则中详述的授权和重新授权要求。

应留存相关文件,包括批准、临时报警和程序以及重新授权的细节。

14.3.3 关于报警搁置的建议

对被搁置超过单个操作轮班的报警应进行审查,对搁置报警的审查要求应记录在报警原则中。

14.3.4 报警搁置记录要求

对每个被搁置超过单个操作轮班的报警,应记录以下信息:

a) 报警标识名；
b) 报警的标签说明或报警描述；
c) 搁置原因。

14.4 操作员的巩固培训

14.4.1 操作员的巩固培训要求

报警的培训要求应根据报警的分类和报警原则中对于不同分类的具体要求来确定。

14.4.2 高度管理报警的巩固培训文档

如果使用了高度管理的报警分类，则应记录以下培训信息：
a) 接受培训的人员；
b) 培训方法；
c) 培训日期；以及
d) 培训历史。
培训频率应在报警原则中明确。培训的相关文件应按报警原则或公司政策规定的周期进行留存。

14.4.3 高度管理的报警的巩固培训内容

如果使用了高度管理的报警分类，应定期对操作员针对每一个高度管理的报警的特征进行培训。巩固培训的内容应包括：
a) 报警的合理化信息；以及
b) 报警的有声和视觉指示。

14.4.4 关于报警巩固培训的建议

操作员应接受涉及报警反应程序的巩固培训，培训应涵盖广泛的过程场景。培训应包括：
a) 报警的合理化信息；以及
b) 报警的有声和视觉指示。
应留存巩固培训的相关记录，表明谁接受了培训，以及接受培训的时间。

15 维护

15.1 目的

维护是报警管理生命周期的一个单独阶段。第15章涵盖了报警系统测试、更换同类产品和维修的相关要求。它描述了报警从正常状态到停用状态再恢复至正常状态之间的转换。维护也需要对维护报警系统的人员进行巩固培训。

15.2 定期报警测试

15.2.1 综述

定期报警测试要求应根据报警的分类和报警原则中对于不同分类的具体要求来确定。定期测试的目的是确保报警持续按照设计运行。

15.2.2 定期报警测试要求

进行测试后,测试记录应按报警原则规定的周期进行留存。记录应包括以下内容:

a) 测试日期;

b) 测试或检测人员的姓名;

c) 设备的唯一标识符(例如:回路编号、位号和设备号);

d) 测试的结果(例如,测试前、后的状态);

e) 关于所使用的测试程序和方法的参考;以及

f) 测试失败的原因。

如果报警原则要求定期对某些报警进行测试,那么报警原则应提供关于测试频率和方式的指南。

15.2.3 高度管理报警的定期测试

如果使用了高度管理的报警分类,属于这些类别的报警应定期进行测试以确保性能。

在高度管理的报警定期测试中发现的任何缺陷应及时修复,否则应立即设置临时报警或程序就位。

15.2.4 定期报警测试程序要求

应为需要测试的报警提供测试程序。

15.2.5 关于定期报警测试程序的建议

程序应包含:

a) 在测试之前停用报警以及在测试之后将报警恢复运行的步骤;

b) 关于可能受测试影响的控制回路或执行单元的适当警告;

c) 如果适用,测试高级报警技术的步骤。

15.2.6 关于定期报警测试的建议

测试记录应包含以下内容:

a) 测试方法;以及

b) 计划的下次测试之前的时间间隔。

定期报警测试中发现的任何缺陷都应及时修复。

15.3 停用报警

15.3.1 综述

关于停用程序的要求应根据报警原则中对于不同报警分类的具体要求来确定。

15.3.2 停用流程要求

长期停用的报警(例如:数日、数周或数月)应被检查以确定是否需要临时报警或程序。

应使用授权和记录流程(例如:许可流程)来停用某个报警。

应针对每一个停用报警记录以下信息:

a) 报警的标识名;

b) 报警类型;

c) 批准细节;

d) 如需要,临时报警或程序的详细信息;以及

e) 停用报警的原因。

15.3.3 停用高度管理的报警

如果某个高度管理的报警停用,应根据风险降低要求和工厂状态,确定适当的临时报警或程序。

15.3.4 关于停用流程的建议

在报警原则中应规定停用报警的审批要求。相关记录的留存时间应在报警原则中进行明确。

15.3.5 报警恢复运行的要求

在将停用报警恢复到运行状态之前,应通知操作员,确保他们知悉报警已恢复以及相关临时措施已移除。

当原始报警恢复运行时,相关临时报警和程序(如适用)应予以移除。

15.4 设备维修

操作员应该可以获得与报警故障相关的信息。如果在报警原则规定的合理时间内不能恢复,因设备功能丧失(例如:因维修或预防性维护而停用的设备)而受到影响的报警应被停用。

15.5 设备更换

现场变更管理程序应关注将改变报警属性的替换设备(例如:测量设备、阀门、工艺设备)。如果进行了更换,则需要根据报警原则中关于该报警分类的具体规定进行报警验证。

15.6 维护的巩固培训

15.6.1 一般要求

报警维护的巩固培训要求应根据报警原则中对于不同报警分类的具体要求来确定。

15.6.2 高度管理的报警的巩固培训要求

如果使用了高度管理的报警分类,应定期对人员针对所有高度管理的报警进行维护要求方面的培训。培训频率应在报警原则中进行规定。培训相关文档应根据报警原则或公司政策规定的周期进行留存。

15.6.3 关于报警的巩固培训的建议

维护人员应接受关于报警维护要求的巩固培训。应留存巩固培训的相关记录,表明谁接受了培训,以及接受培训的时间。应进行评估以确保维护人员对现场维护程序有清晰的理解。

16 监测和评估

16.1 目的

监测和评估是报警管理生命周期的一个单独阶段。这个阶段验证设计、实施、合理化、运行和维护是否符合要求。第16章就使用报警系统分析进行持续监测和定期绩效评估提供了指导。这些活动使用许多相同类型的措施。建议在报警原则中采用若干性能指标。

通过报警系统监测发现的问题可以根据问题的性质在生命周期的几个不同部分(例如:设计、维护

或变更管理)中解决。

16.2 相关要求

报警系统性能应当进行监测。根据报警原则中的目标性能水平,实施报警系统性能的监测和评估。

16.3 监测、评估、审查和基准测试程序

文中将使用监测、评估、审查和基准等术语。

——监测是报警系统性能的定量(客观)方面的测量和报告。

——评估是将监测信息和其他定性(主观)度量的信息与规定的目标和确定的性能指标进行比较。

——审查是一项综合评估,包括评估用于管理报警系统的工作实践的有效性。

——基准测试程序是对报警系统进行初步审查,旨在明确问题区域,以便制定改进计划。

监测通常比进行评估的频率更高,对报警系统性能的某些方面的监测是基于连续的测量。监测的目的是发现问题并采取纠正措施来解决问题。

评估流程的重点是应用工程评价和评估来确定系统是否运行良好。对报警系统相关的工作流程的评估在第18章进行介绍。

16.4 报警系统监测

性能监测是控制和改进的基础。由于传感器老化和过程条件改变或者如果报警变更管理政策不到位,报警系统性能可能会随着时间的推移而退化。持续进行的性能测量可以确定何时需要纠正措施。

当报警经合理化和设计并消除了滋扰报警(例如:抖动报警)后,报警率反映了控制系统使过程保持在操作限内而不需要操作员人工介入的能力。高报警率的解决方案可以包括对控制系统或过程的改进,而不是对报警系统的调整。增强级或高级报警技术可能是必要的。

16.5 报警系统性能指标

16.5.1 综述

各种类型的报警系统分析、关键性能指标和方法都可能被采用。初始报警系统评估和持续监测应包括表7所示的测量。所选分析的整个清单应反映报警原则中做出的决定。

一个典型报警系统中的两类数据是报警记录(即动态或实时数据)和报警属性(即报警设置或组态数据)。这两类数据在报警系统性能测量中都是有价值的,受到不同的分析:

a) 报警记录包含报警相关信息,在报警发生时由系统产生。

b) 报警属性组成了生成报警记录所需的基本结构,包括报警类型、报警设定值、优先级、死区和其他类似项目。

一般而言,至少需要30天的数据来计算各种指标。对于批处理操作,对应于几个相似批次的数据更适用。

下面描述的目标指标是近似的,取决于许多因素(例如:过程类型、操作员技能、人机界面、自动化程度、运行环境、产生的报警的类型和重要性)。根据这些因素,最大可接受的数字可能会显著降低或略高一些。单独的报警率并不是可接受性的一个指标。

16.5.2 每个操作员控制台的平均报警率

报警率(即发出的报警率)的分析是报警系统整体健康状况的一个良好指标。表5中给出了基于一个月数据的每个操作员控制台的平均报警率(即单个操作员的控制和报警责任范围)的推荐目标。这些

频率基于操作员的能力和检测报警、诊断工况、采取纠正措施进行响应并监测工况以验证异常工况已得到纠正所需要的时间。

表 5　平均报警率

很可能可接受	可管理的最大值
每天 144 个报警	每天 288 个报警
每小时 6 个报警(平均)	每小时 12 个报警(平均)
每 10 min 1 个报警(平均)	每 10 min 2 次报警(平均)

持续运行在高于可管理的最大值水平表明一个报警系统发出的报警超过了操作员能处理的量,错过报警的可能性增加。

在某一时间产生的报警超过操作员能处理的量,会增加错过报警的可能性,即使按时间段的平均值来看是可接受的。

16.5.3　每个操作员控制台的峰值报警率

在 10 min 内发生 10 次或 10 次以上的报警,可能会超出操作员的有效报警响应能力,或者导致错过某些报警。在 10 min 内接近 10 个报警的频率是操作员不能长期承受的。

对于峰值报警率分析,通常计算 10 min 时段内(例如:13∶00 至 13∶09)发出的报警。一个月的数据对应的推荐目标是,包含 10 个以上报警的这种 10 min 时段少于 1%。

应同时考虑峰值和平均报警率,因为单独考虑这两种测量方法时都可能具有误导性。应报告超过 10 个报警的时间段数量和最高峰值的具体数值。

16.5.4　报警泛滥

报警泛滥是可变时间段内报警率可能超过操作员的响应能力的报警活动。在报警泛滥中,报警系统对于操作员的辅助作用可能无效。

报警泛滥计算包括确定报警率较高的相邻时间段,从而产生整体泛滥事件。

第一个每 10 min 超过 10 个报警的 10 min 时间段表明一次报警泛滥的开始,第一个每 10 min 小于 5 个报警的 10 min 时间段表明一次报警泛滥的结束。报警泛滥的持续时间应较短,报警总数应较少。作为推荐的目标,报警系统处于泛滥的时间应少于 1%。

对报警泛滥的分析可指出报警系统和过程操作的改进机会。没有提供关于这些指标的目标。报警泛滥分析应包括:

a)　报警泛滥的数量;

b)　每次报警泛滥的持续时间;

c)　每次报警泛滥中的报警计数;以及

d)　每次报警泛滥的峰值报警率。

高级报警技术可以减轻报警泛滥,报警泛滥可能需要高级方法来解决。这些技术在第 12 章中进行了描述。

16.5.5　频繁发生的报警

相对较少的个别报警(例如:10 个至 20 个报警)经常产生报警系统总负荷的较大部分(例如:20%至 80%)。应定期检查最频繁的报警(例如:每日、每周或每月),通过解决最频繁的报警可以大大提高

报警系统性能。

分析方法是使用至少几周的数据，并将报警记录从最频繁到最不频繁排列。最频繁的报警很可能没有正确工作或按照设计工作，高频次的报警往往对其他性能测量有重大的偏移影响。

最频繁的十大报警应占整个系统负荷的一小部分（例如：1%至5%），基于此分析的行动步骤包括针对报警功能正确性和设计的审查。

16.5.6 抖动和瞬时报警

抖动报警在短时间内在报警状态和正常状态之间反复转换，瞬时报警是不会立即重复的类似的短期报警。在这两种情况下，转换不是由于操作员动作的结果。

报警在1 min内重复三次或以上的抖动阈值常被用作最差抖动报警的第一识别标志。也可以使用其他值。

一个抖动报警可能会在几个小时内生成数百或数千条记录，这会明显干扰操作员。抖动报警常在最频繁报警的列表中排名前列。抖动和瞬时报警行为应被消除。不存在长期可接受的抖动和瞬时报警数量。

16.5.7 陈旧报警

连续激活超过24 h的报警可以被认为是陈旧报警。高级报警技术可以用来消除陈旧报警。

陈旧报警不应超过5个。

16.5.8 警报优先级分布

有效地使用报警优先级可以提高操作员管理报警和提供响应的能力。报警优先级的有效性与报警优先级的分配有关：较高的优先级应更少被使用。

一些报警系统针对少数对应严重后果的报警使用一个附加的最高优先级。

附加的优先级可能是有用的，例如，针对操作员动作非常有限的仪表诊断报警的最低优先级。对于诊断报警，没有建议的频率或百分比分配，因为没有建议的仪表故障频率，越低越好。

在特殊情况下，有时会使用针对各种受限警报（例如：无声报警）的优先级。对于针对受限警报的优先级，没有建议的分布比例。

与这些推荐比例严重偏离的警报优先级分布可能降低优先级的价值，并且通常表明报警优先级设置没有遵从一致的报警合理化方法。有效的合理化是通常的解决方法。

16.5.9 报警优先级分配

有效的报警合理化将产生类似于表6的警报优先级分布。警报优先级分布不等同于合理化的报警优先级分布，因为不是所有报警都有相同的发生可能性。对于不准许对仪表或系统诊断报警进行优先级分级的报警系统，可以将这些报警排除在优先级分布计算之外，以避免得到曲解的分布。

表6 警报优先级分布

优先级名称	比例分布
3个优先级：低、中、高	～80%低、～15%中、～5%高
4个优先级：低、中、高、最高	～80%低、～15%中、～5%高、～<1%最高

16.6 未经授权的报警抑制

搁置、依据设计抑制和停用状态都是作为受控的方法所预期的报警状态。在这些方法之外，报警也

有可能被抑制,应检测并报告未经授权的报警抑制,出错的可能性和由此产生的风险是很高的。

报警状态转换至抑制状态以及从抑制状态转换至其他状态都应进行记录。应利用分析方法检测和报告这些方法之外被抑制的报警。在没有授权的情况下,不应有报警被抑制。

16.7 报警属性监测

应通过将实际报警属性与合理化信息进行对比,检测并解决未授权的报警属性变更。差异应迅速确认和解决。未经授权的报警更改的目标值为零。

16.8 报警系统分析报告

报警系统分析应以适当的频率报告给予报警系统相关的人员(例如:操作员、员工和经理)。

在一项改进工作的各个阶段,应在不同的报告阶段进行不同的分析(例如:在开始阶段提供周报,之后提供月报)。每周分析也可以涵盖前 30 天的数据,以产生有意义的趋势。报警原则应指定分析和报告频率。

应对报警分析识别出的问题采取行动,并定期报告行动的进展和状态。

16.9 报警性能指标汇总

前面描述的报警性能指标和示例目标值(具有相同资格的)汇总如表 7 所示。

表 7 推荐的报警性能指标汇总

基于至少 30 天数据的报警性能指标		
指标	目标值	
每次发出的报警数量	目标值:很可能是可接受的	目标值:可管理的最大值
每个操作员控制台每天发出的报警	每天 144 次报警	每天 288 次报警
每个操作员控制台每小时发出的报警	~6(平均)	~12(平均)
每个操作员控制台每 10 min 发出的报警	~1(平均)	~2(平均)
指标	目标值	
包含超过 30 个报警的小时数百分比	~< 1%	
包含 10 个以上报警的 10 min 时间段的百分比	~< 1%	
10 min 时间段内的最大报警数	≤ 10	
报警系统处于泛滥状态的时间百分比	~1%	
前 10 个最频繁的报警占整体报警负荷的百分比	最大 1%到 5%,有相关行动计划,以解决缺陷	
抖动和瞬时报警的数量	0,有相关行动计划,以纠正发生的任何抖动和瞬时报警	
陈旧报警	每天少于 5 次,并有相关行动计划	
警报优先级分布	3 个优先级:~ 80%低,~ 15%中,~ 5%高,或 4 个优先级:~ 80%低,~ 15%中,~ 5%高,~ < 1%最高 排除在计算之外的其他特殊用途的优先级(例如:系统诊断报警)	
未经授权的报警抑制	不准许任何报警在受控的或批准的方法之外被抑制	
未经授权的报警属性变更	不准许任何报警属性在受控的或批准的方法之外被更改	

17 变更管理

17.1 目的

变更管理是生命周期的一个单独阶段。第17章涵盖了关于报警系统变更的要求，包括添加新的报警、删除现有报警、报警属性修改、授权和相关文档。变更管理的目的是确保变更经过了授权并满足报警原则中描述的评估标准。变更管理流程确保将适当的生命周期活动应用于报警系统。

17.2 经受变更管理的修改

报警的添加或删除，以及对特定属性的修改，需要通过变更管理程序进行授权。对导致报警设定值、分类、优先级、后果、依据、抑制逻辑或响应时间与授权值不同的永久性变更，需要通过变更管理程序进行评估。

变更管理程序应确保解决以下问题：

a) 拟议变更的技术基础；
b) 变更对健康、安全和环境的影响；
c) 修改符合报警原则；
d) 操作程序的修改；
e) 变更的有效时间；
f) 拟议变更的授权要求；
g) 如果拟议变更的报警是出于安全原因实施的报警，安全度得以维持；
h) 审查中包括适当学科的人员；
i) 对报警系统的更改应遵循所有适当的后续报警管理生命周期活动；以及
j) 所有变更的实施遵守报警原则中规定的程序。

17.3 变更文档要求

文档要求应根据报警的分类和报警原则中对于不同分类的具体要求来确定。

针对批准的变更，下列信息应进行记录：

a) 变更原因；
b) 变更日期；
c) 实施变更的人员的姓名；
d) 授权变更的人员的姓名；
e) 变更的性质(即之前和之后)；
f) 培训要求；
g) 测试要求。

17.4 关于变更文档的建议

由报警变更引起的对相关系统组件和文档的更改应记录为变更记录的一部分。记录应：

a) 防止未经授权的修改、破坏或丢失；
b) 在适当的文件控制程序的控制下进行修订、修改、审查和批准；
c) 根据现场记录保存政策确定的时长进行存储；
d) 按照报警原则对于不同分类的要求进行维护。

17.5 关于报警移除的建议

如果不再需要某个报警，则应将其从报警系统中移除。显示和相关文件应在合理的时间内修改。

17.6 关于报警属性修改的建议

应当生成并维护一系列参考资料（例如：图形、控制逻辑、P&ID、操作程序和 HAZOP）。在变更报警之前，应回顾上述参考资料。这可以防止在文档中引入不正确的信息，并有助于防止临时自动化逻辑和图形错误。

18 审查

18.1 目的

审查是定期进行的生命周期的一个独立阶段，以维持报警系统和报警管理流程的完整性。对报警系统性能进行审查可以从监测结果中揭示不明显的差距。对报警原则的执行情况进行审查，以识别系统改进需求，例如，修改报警原则或其中定义的工作流程。

审查将审查与报警系统相关的管理和工作实践。通过审查将各种工作程序和政策或要求进行对比，以确定这些做法是否足以充分管理报警系统。审查还包括将报警管理实践与行业指南进行对比。

审查的频率低于监测和评估。

18.2 基准审查程序

18.2.1 综述

报警管理的各个方面都应在改进工作开始时进行审查。应针对一套成文的实践（例如：本文件中列举的实践）建立初始审查或基准审查程序。基准审查程序包括审查流程的初始迭代，以便捕捉工作实践关心的问题。初始审查的结果可以用于编制报警原则。

18.2.2 初始审查或基准审查程序的要求

按照报警分类的要求，所有报警应遵循报警原则中规定的审核频率和具体的审核要求。

审查应符合本文件的所有适用要求。

18.3 审查访谈

人员访谈或问卷调查应作为审查的一部分进行，以识别报警系统性能和可用性问题。访谈主题可能包括：

a) 仅在需要操作员动作的情况下发生报警；
b) 报警优先级的应用遵从了一致性且有意义；
c) 报警发出及时，使得操作员可采取有效的行动；
d) 定义了报警系统用户和支持人员的角色和责任；以及
e) 关于报警系统的使用和功能的培训是有效的。

18.4 关于审查的建议

报警原则应根据行业指南和本文件的要求和建议进行审核。确保符合报警原则的工作流程和程序应定期评估其有效性。审查应审查所有相关文档，可能包括如下：

a) 关于报警要求操作员采取行动以避免确定的后果的验证；
b) 报警属性和合理化的相关文档；
c) 在主报警数据库中修改报警属性的变更管理文档；
d) 报警性能监测报告；
e) 故障报警修复的相关文档；以及
f) 停用报警的相关文档。

18.5 行动计划

应针对在审查过程中发现的问题制定行动计划。当确定一套行动计划时，应为每个分项制定时间轴、职责和结果审查。

参 考 文 献

[1] GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

[2] GB/T 21109.1—2007 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求

[3] IEC 61511(all parts) Functional safety—Safety instrumented systems for the process industry sector

[4] IEC 62241 Nuclear power plants—Main control room—Alarm functions and presentation

[5] IEC 62264-1:2003 Enterprise-control system integration—Part 1: Models and terminology

[6] IEC 62264-2:2004 Enterprise-control system integration—Part 2: Object model attributes

[7] IEC 62541-9 OPC unified architecture—Part 9: Alarms and conditions

[8] Alarm Management, NAMUR-Worksheet NA 102, 3rd Edition, NAMUR-Geschäftsstelle, Leverkusen, Germany (2008)

[9] ANSI/ISA-18.02—2009 Management of Alarm Systems for the Process Industries

[10] Engineering Equipment Materials Users' Association, Alarm Systems—A Guide to Design, Management and Procurement, EEMUA Publication No. 191, 2nd Edition, EEMUA, London, UK (2007)

[11] Engineering Equipment Materials Users' Association, Alarm Systems.—A Guide to Design, Management and Procurement. EEMUA Publication No. 191, 2nd edition. London: EEMUA, 2007

中 华 人 民 共 和 国

国 家 标 准

过程工业报警系统管理

GB/T 41261—2022/IEC 62682:2014

*

中国标准出版社出版发行

北京市朝阳区和平里西街甲2号(100029)

北京市西城区三里河北街16号(100045)

网址:www.spc.org.cn

服务热线:400-168-0010

2022年3月第一版

*

书号:155066·1-68983

GB/T 41261-2022

码上扫一扫 正版服务到