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。

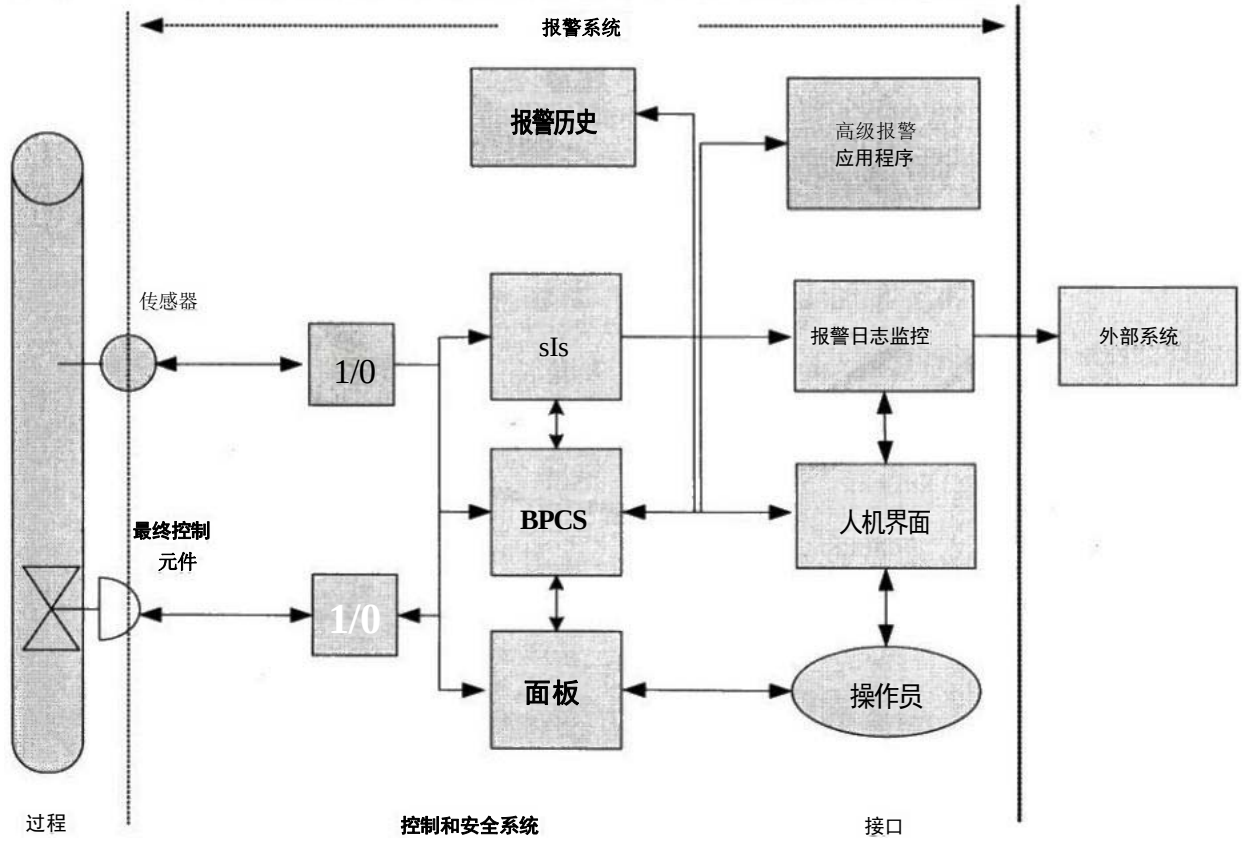


图 1 报警系统数据流

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(dPV/dt) 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)

0OSRV: 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。

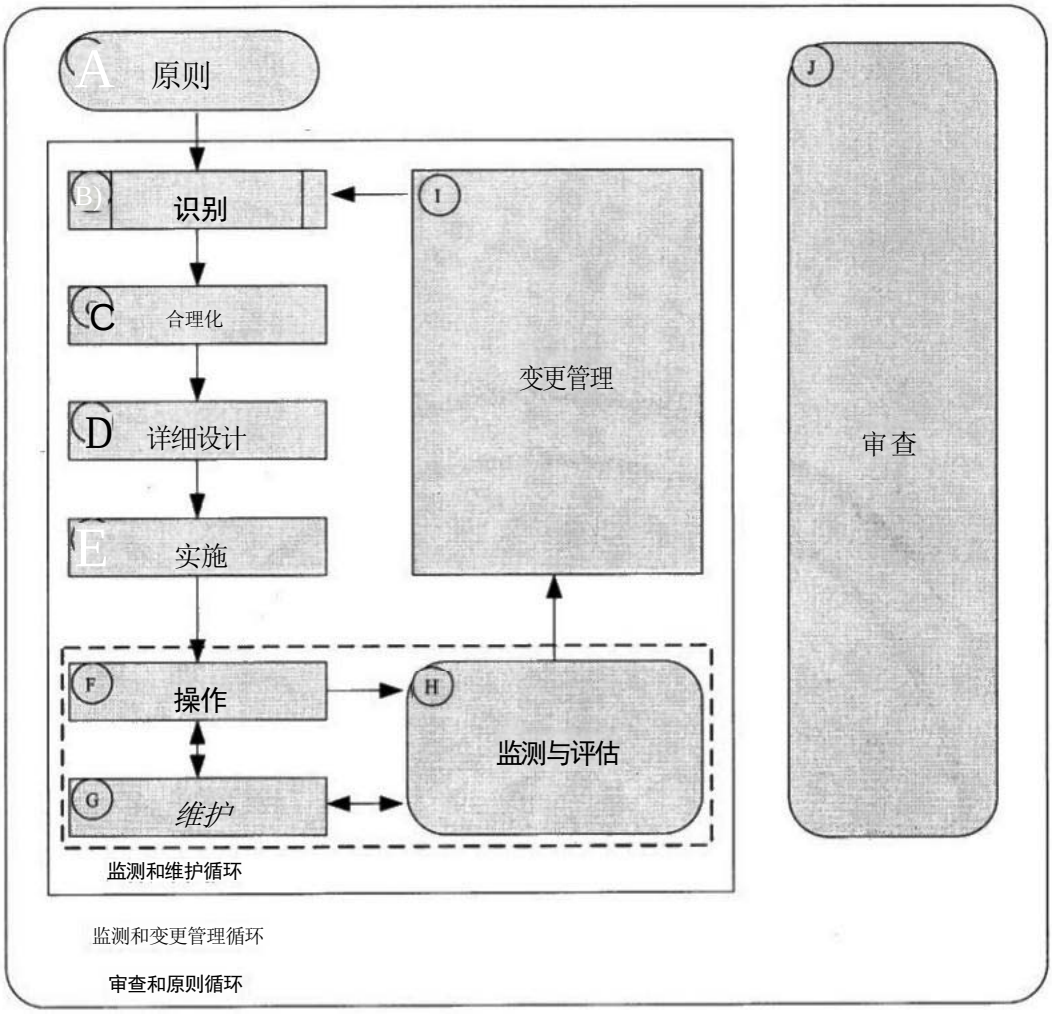
报警管理的基础部分是报警的定义，即通过一种有声和/或可视的方式向操作员指示需要响应的设备故障、过程偏差或其他异常状况，该定义的一个关键要素是对报警的响应。本文件描述的报警管理流程对该定义进行了进一步阐释。

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。

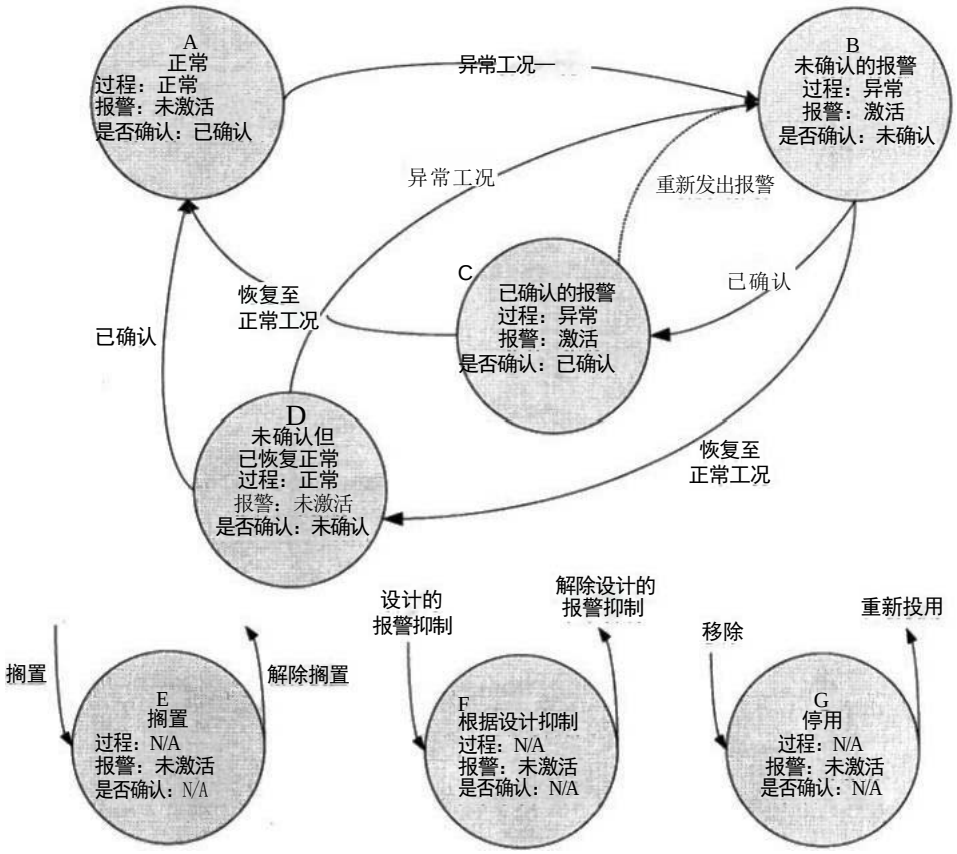
表 1　报警管理生命周期阶段输入和输出

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(0OSRV)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	0OSRV	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。

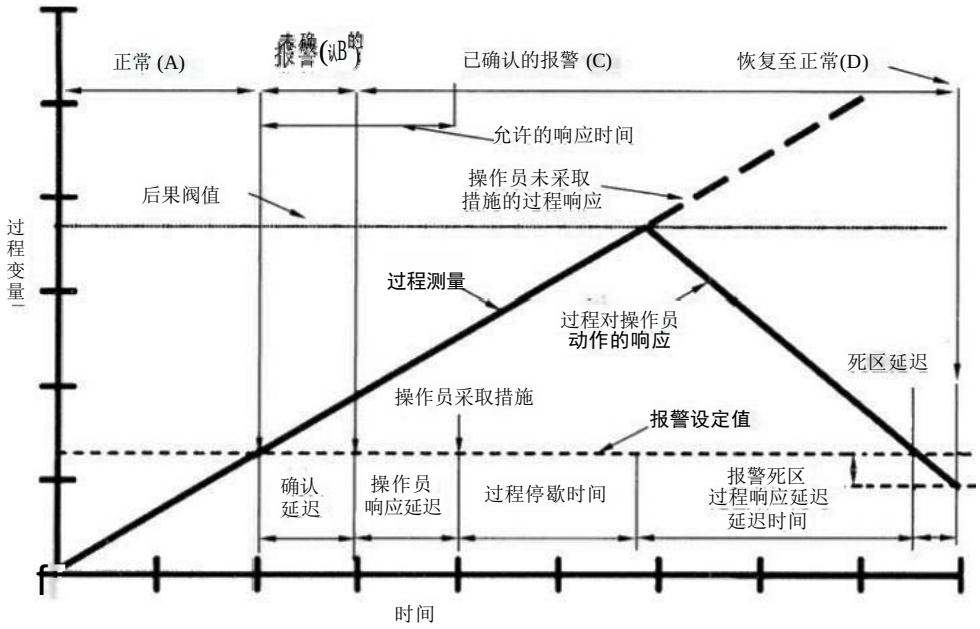


图 4　报警响应时间轴

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。

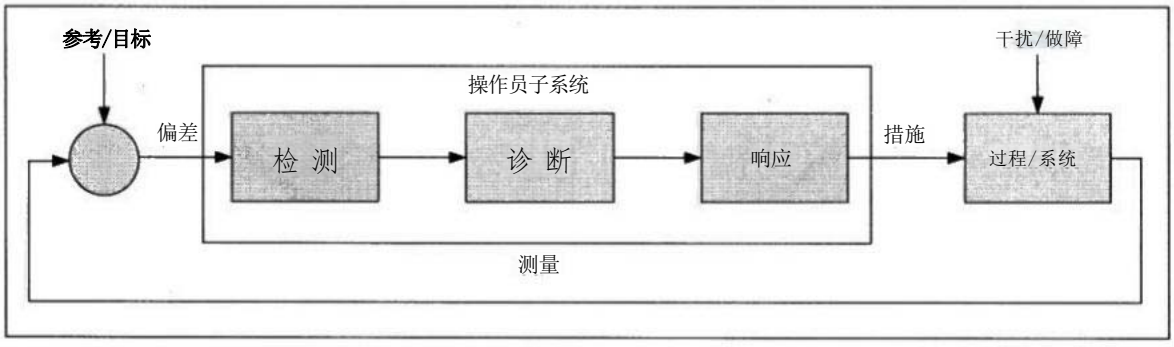


图 5 操作员与过程交互的反馈模型

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；