ICS **.**.**
P **
备案号：

SH

中华人民共和国石油化工行业标准

SH/T 3245—202x

石油化工报警管理系统设计规范

Design specification for alarm management system in petrochemical industry

（报批稿）

202X-XX-XX 发布　　202X-XX-XX 实施

中华人民共和国工业和信息化部　发布

目　次

前　言……V
1　范围……1
2　规范性引用文件……1
3　术语和缩略语……1
3.1　术语和定义……1
3.2　缩略语……5
4　报警管理生命周期……5
4.1　一般规定……5
4.2　报警原则……6
4.3　报警辨识与合理化分析……6
4.4　工程设计与实施……7
4.5　运行、维护与变更管理……7
4.6　性能监测、评估与审查……7
5　设计基本原则……7
5.1　一般规定……7
5.2　报警管理系统设计原则……8
6　报警分级……8
6.1　一般规定……8
6.2　报警分组……9
6.3　报警分类……9
6.4　报警优先级划分……10
7　报警管理系统……10
7.1　功能要求……10
7.2　硬件要求……11
7.3　软件功能……11
7.4　通信接口……11
7.5　网络配置与安全……11
8　报警人机界面……12
8.1　一般规定……12
8.2　报警管理系统人机界面……12
8.3　报警系统人机界面……13
9　工程设计与实施……13
9.1　工程设计……13
9.2　工程实施……14
10　运行、维护与变更管理……14
10.1　运行……14
10.2　维护……15
10.3　变更管理……15
11　性能监测、评估与审查……16
11.1　报警性能监测……16
11.2　报警性能评估……16
11.3　审查……16

附　录　A　（资料性）报警系统关键性能指标（KPI）……18
附　录　B　（资料性）报警优先级划分评估典型工作流程……19
附　录　C　（资料性）报警优先级划分评估方法……20
参　考　文　献……22
本规范用词说明……23
附：条文说明……24

石油化工报警管理系统设计规范

1 范围

本规范规定了石油化工报警管理系统工程设计的原则和要求。

本规范适用于石油化工和以煤为原料制取燃料及化工产品工厂的新建、扩建和改建工程的报警管理系统的工程设计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本规范必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本规范；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB/T 32857	保护层分析（LOPA）应用指南
AQ/T 3054	保护层分析（LOPA）方法应用导则
SH/T 3092	石油化工分散控制系统设计规范

3 术语和缩略语

3.1 术语和定义

下列术语和定义适用于本规范。

3.1.1

报警 alarm

通过声响和/或视觉显示的方式警告或提示操作员出现了过程参数偏离设定值、工艺设备故障、仪表及控制系统诊断故障或其他异常情况，提醒操作员在特定时间内进行响应操作。

3.1.2

过程报警 process alarm

报警的一种类型。由于过程参数偏离设定值或工艺设备故障等异常情况产生的报警。

3.1.3

报警率 alarm rate

每位操作员在特定的时间间隔内接收的报警次数。

3.1.4

报警泛滥 alarm flood

报警率超过操作员能够有效管理的一种状态。

3.1.5

报警系统 alarm system

由一系列硬件与软件构成的系统，用于检测和生成报警并警告或提示给操作员，同时记录、存储报警信息和响应操作情况。

3.1.6

报警管理 alarm management

针对报警和报警系统进行的报警原则制定、文档记录、设计、操作、监视和维护等一系列的工作流程和实践活动。

3.1.7

报警管理生命周期 alarm management lifecycle

包括报警原则制定、报警辨识、合理化分析、工程设计、工程实施、运行、维护、变更管理、性能监测与评估、审查等阶段的报警管理活动的总称。

3.1.8

报警管理系统 alarm management system

通过软硬件接口，读取报警系统中的实时报警信息，并基于软件平台技术，辅助实践报警生命周期管理各阶段工作，使报警系统的报警率符合相关标准规范要求，提升操作维护人员对报警的响应与处理能力。报警管理系统也称为先进报警管理系统（advanced alarm-management system）。

3.1.9

报警抑制 alarm suppress

当报警被激活时，阻止其向操作员发出报警警示。报警抑制可分为手动抑制、自动抑制。

3.1.10

手动抑制 manual suppress

当报警被激活时，由操作员手动发起的临时性报警抑制，经过预设的时间后自动解除抑制，或在预设的时间内由操作员手动解除抑制。手动抑制期间报警记录功能仍然有效。

3.1.11

自动抑制 automated suppress

当报警被激活时，根据装置运行状态或其他条件自动发起的临时性报警抑制，在状态或条件消失后依设定程序自动解除抑制。自动抑制期间报警记录功能仍然有效。

3.1.12

报警停用 alarm disable

在长期维修或不使用期间，暂时停用报警功能，可在需要时手动恢复。在报警停用期间，即使过程变量达到报警设定值，报警不会被激活，也不会进行报警记录。

3.1.13

最大允许响应时间 maximum allowable response time （Tmar）

从报警产生到操作员通过正确响应操作使过程参数在达到安全联锁或其他保护动作阈值之前向安全方向转变之间的最长时间间隔。

3.1.14

报警优先级 alarm priority

根据报警的后果严重程度和最大允许响应时间对报警进行的分级，表示报警级别的差异。报警优先级越

高，代表报警重要性和响应紧迫性越高。

3.1.15

报警死区 alarm deadband

报警设定值与报警退出值之间的回差区域。

3.1.16

报警延迟 alarm on-delay

过程变量达到报警设定值至报警报出之间的时间延迟。

3.1.17

报警解除延迟 alarm off-delay

过程变量恢复到报警设定值之内的正常状态至报警退出之间的时间延迟。

3.1.18

首出报警 first-out alarm

在多个报警场景下被确定（通过首出逻辑分析）最先发出的报警。

3.1.19

偏差报警 deviation alarm

两个或多个过程变量测量值的偏差超过限值的报警。

3.1.20

自适应报警 adaptive alarm

通过算法自动改变报警设定值的报警。

3.1.21

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。

3.1.22

统计报警 statistical alarm

基于对一个或多个过程参数的统计处理结果而生成的报警。

3.1.23

抖动报警 chattering alarm

短期内在激活状态和非激活状态（正常状态）之间重复转换的报警。

3.1.24

瞬时报警 fleeting alarm

某个报警报出后，在极短的时间内恢复正常。通常在报出后1秒之内恢复正常状态的报警可定义为瞬时报警。

3.1.25

陈旧报警 stale alarm

报警长时间得不到解除的报警。通常超过24小时未解除的报警可定义为陈旧报警。

3.1.26

变化率报警 rate-of-change alarm

单位时间内过程参数的变化率超过预先设定的数值时产生的报警。

3.1.27

位模式报警 bit-pattern alarm

当数字信号的值与预先设定的状态值相匹配时产生的报警。

3.1.28

状态偏差报警 discrepancy alarm

预期状态与实际状态之间出现差异时产生的报警。

3.1.29

重新触发报警 re-triggering alarm

在一定条件下自动重新发出的报警。

3.1.30

坏值报警 bad value alarm

模拟量输入值超出正常检测限值一定程度时，产生坏值报警。坏值报警属于仪表故障诊断报警。

3.1.31

滋扰报警 nuisance alarm

不必要的、过度的或在操作员做出正确响应操作之后仍无法恢复到正常状态的报警。滋扰报警通常包括抖动报警、瞬时报警、陈旧报警等。

3.1.32

提醒 alert

通过有别于报警的声响和/或视觉显示，提醒操作员在时间允许时进行评估或处理的信息。

3.1.33

事件 event

控制系统、操作及各类动作触发的记录

3.1.34

控制系统 control system

对来自过程和/或操作员的输入信号进行响应，并产生使过程以期望的方式运行的输出信号的系统。控制系统包括基本过程控制系统（BPCS）、安全仪表系统（SIS）、气体检测报警系统（GDS）等。

3.1.35

基本过程控制系统 basic process control system

响应过程测量及其他相关设备、仪表、控制系统或操作员的输入信号，按过程控制规律、算法、方式，产生输出信号实现过程控制及其相关设备运行的系统。基本过程控制系统包括分散控制系统（DCS）、压缩机控制系统（CCS）、可编程逻辑控制器（PLC）、数据采集与监控系统（SCADA）等。

3.2 缩略语

下列缩略语适用于本规范。

AAS	Alarm Management System	报警管理系统
	(or Advanced Alarm-management System)	（也称先进报警管理系统）
BPCS	Basic Process Control System	基本过程控制系统
CCS	Compressor Control System	压缩机控制系统
CPU	Central Processing Unit	中央处理单元
DCS	Distributed Control System	分散控制系统
FAT	Factory Acceptance Test	工厂验收测试
FDS	Functional Design Specification	功能设计规格书
GDS	Gas Detection and alarm System	气体检测报警系统
HAZOP	Hazard and Operability Study	危险与可操作性分析
HMI	Human Machine Interface	人机界面
HSE	Health, Safety and Environment	健康、安全和环保
IFAT	Integrated Factory Acceptance Test	工厂集成验收测试
KPI	Key Performance Indicator	关键性能指标
LOPA	Layer of Protection Analysis	保护层分析
MES	Manufacturing Execution System	生产管理系统
MOC	Management of Change	变更管理
OPC	OLE for Process Control	用于过程控制的对象链接与嵌入
P&ID	Piping and Instrumentation Diagram	工艺管道及仪表流程图
PLC	Programmable Logic Controller	可编程逻辑控制器
SCADA	Supervisory Control And Data Acquisition	数据采集与监控系统
SIL	Safety Integrity Level	安全完整性等级
SIS	Safety Instrumented System	安全仪表系统
SRS	Safety Requirements Specification	安全要求规格书
UPS	Uninterruptable Power Supply	不间断电源

4 报警管理生命周期

4.1 一般规定

4.1.1 应确定并开展报警管理生命周期内各阶段所需的管理活动和技术活动。

4.1.2 报警管理生命周期宜分为工程建设阶段和运行维护阶段。

4.1.3 报警管理生命周期活动宜包括报警原则制定、报警辨识、合理化分析、工程设计、工程实施、运行、维护、变更管理、性能监测与评估、审查等，如图4.1.3所示。

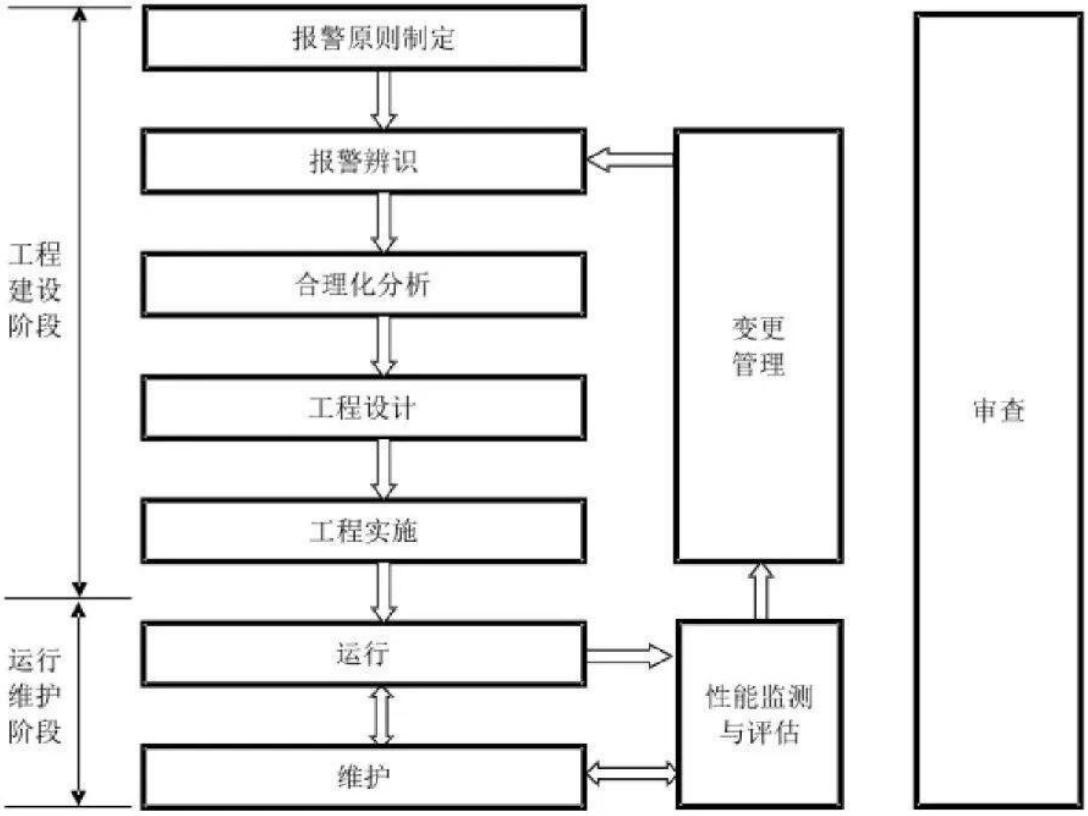

图4.1.3 报警管理生命周期各阶段的典型活动

4.2 报警原则

4.2.1 报警原则应根据企业特点制定，工厂或装置的报警设置原则和管理规程应保持一致。

4.2.2 报警原则应作为开展报警管理生命周期各阶段活动的依据。

4.2.3 报警原则宜包括以下内容：

a) 报警管理系统（AAS）的目标、功能以及相应的工作流程；

b) 报警管理所需的管理岗位及其职责范围；

c) 报警设置原则，包括报警设计基本原则、报警分级技术要求、报警设定值确定原则、报警延迟和报警死区设置原则、报警抑制和报警停用设置原则、报警人机界面功能要求等；

d) 报警管理系统以及相关硬件、软件的日常维护、测试的原则和要求；

e) 工程设计、工程实施、运行、维护、变更管理、性能监测与评估、审查等阶段的活动要求，及各阶段的培训、文档等要求。

4.3 报警辨识与合理化分析

4.3.1 报警辨识宜基于危险与可操作性分析（HAZOP）、保护层分析（LOPA）、安全要求规格书（SRS）、工艺管道及仪表流程图（P&ID）、事故调查报告、工程及生产实践经验、工艺操作手册等完成。报警辨识确定的报警及报警参数应作为合理化分析的输入信息。

4.3.2 合理化分析宜包括报警和报警设定值设置的合理性、报警原因、报警后果严重程度、报警最大允许响应时间、报警优先级、操作员响应操作、报警分组、报警分类等。

4.3.3 合理化分析的结果应进行归档，作为报警管理系统工程设计和工程实施的依据。

4.4 工程设计与实施

4.4.1 报警管理系统的工程设计应在完成报警辨识和合理化分析后实施，工作包括确定报警、报警设定值、报警分类、报警死区、报警延迟、人机界面等。

4.4.2 报警管理系统的集成、组态、调试和验收等工程实施工作应根据报警管理系统工程设计相关文件开展，确保实现规定的功能。

4.5 运行、维护与变更管理

4.5.1 报警管理系统在投入运行前应制定报警管理规程，设置合理的管理组织并明确岗位职责分工，投入运行后应按照各项管理规程进行日常管理、持续改进报警管理水平，并加强对报警管理相关人员的培训。

4.5.2 报警管理系统运行过程中应持续进行维护工作，如报警定期测试、报警设备维修等，保证报警管理系统正常运行。

4.5.3 为保证报警管理系统的完整性和有效性，应建立报警管理生命周期内的变更管理规程，有效管理报警变更。变更管理宜包括申请、评估、审查、批准、实施、培训、监督等流程。

4.6 性能监测、评估与审查

4.6.1 报警管理系统应能对报警系统的性能进行持续监视与检测，以量化指标进行汇总展示。

4.6.2 报警管理相关人员应定期对报警系统的性能监测结果进行评估。对于需要改进提升的问题，应提出解决方案并按照管理规程及职责分工进行落实解决。

4.6.3 审查活动贯穿整个报警管理生命周期，应定期审查报警管理系统和报警系统的性能及管理活动的完整性和有效性。对于审查过程中发现的问题，应制定整改计划并落实解决。

5 设计基本原则

5.1 一般规定

5.1.1 设置报警的目的应为提醒操作员关注出现的异常事件并且进行响应操作，防止可能发生严重的工艺波动、意外停车或重大事故。不需要操作员响应操作的事件不应设置报警和纳入报警管理。

5.1.2 报警的设置应合理，对于某个异常事件不应同时设置多个表示相同含义的报警。设置的报警应反映异常事件发生的根本或主要原因，报警信息应唯一、及时和有效。

5.1.3 报警设定值的确定应合理并充分考虑相关的逻辑关系。确定报警设定值时，既应留给操作员足够的响应操作时间，又不宜设置得过于保守而造成频繁报警，干扰正常的生产操作。

5.1.4 报警分级应遵循统一的原则，且应有预设的响应机制。报警优先级在工艺波动严重或报警泛滥时将直接决定操作员响应操作的优先顺序，即操作员应先响应高优先级的报警。

5.1.5 提示操作员的报警信息宜具有统一的表述方式且简洁清晰。

5.1.6 操作员对报警进行核实、评估和响应操作应遵循统一的规程。

5.1.7 当报警及其操作员响应操作作为独立保护层时，相关报警应符合GB/T 32857和AQ/T 3054的规定，并宜划分为最高优先级。

5.1.8 在基本过程控制系统（BPCS）中宜设置安全仪表系统安全联锁动作前的预先报警。

5.1.9 典型的报警系统关键性能指标（KPI）见附录A，报警率宜控制在操作员能有效处理的范围内。

5.1.10 报警不应取代操作员操作和监控。

5.2 报警管理系统设计原则

5.2.1 报警管理系统应建立所有报警信息的报警数据库，定期归档记录，便于查询、审查和培训。

5.2.2 报警管理系统的设计应兼顾安全性、可用性、可维护性、可追溯性和经济性。

5.2.3 报警管理系统的硬件、应用软件、操作系统等应采用正式发布版本。

5.2.4 报警管理系统应采用UPS供电。

5.2.5 报警管理系统应与基本过程控制系统采用同一时钟源。

5.2.6 报警管理系统宜采用服务器完成报警分析和历史报警管理。报警管理系统的客户端可与基本过程控制系统中其他高级应用的客户端共用。

5.2.7 报警管理系统服务器独立设置时，应采取网络信息安全措施，符合工业控制系统网络信息安全要求。

6 报警分级

6.1 一般规定

6.1.1 报警分级可包括报警分组、分类、优先级划分等，报警分级评估应根据报警原则开展。

6.1.2 过程报警分级评估宜包括以下内容：

a) 报警原因；

b) 操作员响应操作；

c) 报警的后果严重程度；

d) 报警最大允许响应时间；

e) 报警优先级。

6.1.3 过程报警分级评估宜在合理化分析阶段完成，报警优先级划分评估典型工作流程见附录B。

6.1.4 在开展过程报警分级评估之前，应准备好所需的资料和数据，并应组织协调相关人员参加。需准备的资料和数据宜包括（但不限于）下列文件：

a) P&ID；

b) 工艺操作手册；

c) 报警原则；

d) 报警管理系统功能设计规格书（若有）；

e) HAZOP、LOPA及SIL分级等报告；

f) 联锁逻辑说明、因果表或逻辑图；

g) 报警和联锁设定值表；

h) 所有报警点的组态数据（若有）；

i) 现场操作规程、事故调查报告（若有）；

j) 报警归档和合理化分析软件工具。

6.1.5 过程报警分级评估参加人员宜包括：

a) 由具有过程报警分级评估分析工作经验的专家主持；

b) 有经验的操作员；

c) 熟悉工艺流程和相关经济指标的工艺工程师；

d) 仪表及控制系统工程师；

e) 安全、环保、设备等相关人员。

6.2 报警分组

6.2.1 报警系统应按照操作岗位进行报警分组，以减少不同操作岗位报警的相互干扰，减轻操作员报警响应操作负荷。

6.2.2 报警分组应与操作岗位的职责范围一致，不应包括与本操作岗位无关的报警。

6.2.3 与操作岗位相关的公用工程单元的报警应分配至相应操作岗位的报警分组，并明确报警响应操作责任。与本操作岗位无关的公用工程报警可作为提醒信息。

6.3 报警分类

6.3.1 报警类型宜分为过程报警、HSE报警和仪表及控制系统诊断报警。

6.3.2 过程报警宜包括如下过程变量：

a) 温度、压力/差压、流量、物位、成分分析、密度、重量、位置等；

b) 振动、位移、转速、轴承/轴瓦/定子温度、键相位、电流、功率等。

6.3.3 过程报警的类型宜分为：

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) 位模式报警；

g) 自适应报警；

h) 重新触发报警；

i) 统计报警；

j) 首出报警。

6.3.4 HSE报警宜纳入过程报警管理范畴。

6.3.5 仪表及控制系统诊断报警应报出智能仪表及控制系统的硬件、软件、其他组件或连接线路的故障，宜与过程报警分开显示汇总。常见的诊断报警类型宜包括：

a) 坏值报警；

b) 仪表诊断报警；

c) 控制系统诊断报警。

6.4 报警优先级划分

6.4.1 报警优先级划分应采用一致性的原则和方法，合理定义报警优先级。

6.4.2 过程报警的后果严重性宜通过HAZOP、LOPA等风险辨识方法，根据报警保护的事故场景确定。后果严重性宜分为级别1（轻微）、级别2（中等）、级别3（较大）、级别4（严重）四个等级，可参考附录C的表C.1。

6.4.3 过程报警的时间紧迫性宜通过最大允许响应时间（T_{mar}）评估。最大允许响应时间宜分为定义不合理、及时响应操作、快速响应操作、紧急响应操作四个等级，可参考附录C的表C.2。对于定义不合理的报警（如T_{mar}>30 min），宜取消报警或重新设置报警参数。

6.4.4 过程报警优先级的确定应根据后果严重性等级和最大允许响应时间等级两个指标确定，宜划分为下列三个优先级，可参考附录C的表C.3：

a) 第一级（紧急）过程报警；

b) 第二级（重要）过程报警；

c) 第三级（一般）过程报警。

6.4.5 涉及人身安全的HSE报警应将其优先级划分为最高优先级报警。

6.4.6 重要的仪表及控制系统诊断报警可纳入过程报警管理范畴，并宜划分为低优先级报警（如一般过程报警）。

7 报警管理系统

7.1 功能要求

7.1.1 报警管理系统应能从报警系统中自动获取报警状态和相关配置参数，并建立报警数据库。报警历史数据保存时间宜大于5年，并可通过文件备份等方式保存更长时间的数据。

7.1.2 报警管理系统应能从基本过程控制系统中读取操作员响应操作的事件记录，涵盖从报警报出到操作员处理完成的全过程。

7.1.3 报警管理系统的报警数据库应具有与报警系统报警设置的对比功能，若有差异，应产生提醒信息。

7.1.4 报警管理系统应具有对报警系统关键性能指标（KPI）、报警泛滥、滋扰报警（如抖动报警、瞬时报警、陈旧报警等）、报警类型、报警优先级、某时间段的报警数量、报警时间、处于报警抑制和报警停用状态的报警数量等数据统计与分析功能。

7.1.5 报警管理系统应能根据用户需求定制各类报表和报告，支持多种输出和打印格式。报表内容可以自定义时间段（如周报、月报等）、自定义装置或单元等，实现差异化报表。

7.1.6 报警管理系统应能根据用户需求定制各类HMI画面，见8.2节的规定。

7.1.7 报警管理系统宜能根据企业需求设置与企业生产管理系统（MES）等外部网络的通信接口，能提供基于网络访问的功能，可在办公网或远程访问查询报警信息，可通过网络实现信息分级推送功能，如推送至电子邮箱、移动设备等。

7.1.8 报警管理系统应具备报警归档与合理化分析的软件功能。

7.1.9 报警管理系统宜具有实时报警管理功能，可在线读取报警系统报警参数，并为报警系统按照报警原则实现报警抑制（如手动抑制、自动抑制）、报警停用、多工况报警等功能提供支持。

7.1.10 报警管理系统应具有在线维护、修改及下装软件功能。

7.1.11 报警管理系统应具备权限管理功能，应能按工程师和操作员等不同安全级别进行管理授权，根据权限设置网络中不同用户浏览或维护的数据范围、内容和使用不同功能。

7.2 硬件要求

7.2.1 报警管理系统由应用服务器和客户端组成， 服务器的硬件配置应能满足数据存储和访问的要求。

7.2.2 对于全厂或规模较大的项目，报警管理系统可单独设置用于数据采集的OPC服务器。

7.2.3 报警管理系统应用服务器的硬盘应冗余设置，服务器的运行负荷不宜高于最大能力的50%。

7.2.4 用于报警管理系统通信的网络交换机带宽宜为千兆级。

7.3 软件功能

7.3.1 报警管理系统软件应包括报警数据采集软件、服务器/客户端软件、数据库软件、人机界面软件和各类功能性软件。

7.3.2 报警管理系统的统计分析软件应满足各类报警分析和报表功能需求。

7.3.3 报警管理系统人机界面软件的风格应与报警系统协调一致，可在线灵活组态修改、查询报警信息。

7.3.4 报警管理系统应具有报警归档与合理化分析工具软件。

7.3.5 报警管理系统宜具有报警实时管理工具软件。

7.3.6 报警管理系统宜具有网络浏览查询及信息推送功能的软件。

7.4 通信接口

7.4.1 报警管理系统宜通过OPC协议采集基本过程控制系统的报警数据，安全仪表系统等其他控制系统的报警信息宜先通信至基本过程控制系统。

7.4.2 报警管理系统在报警数据读取过程中不应影响报警系统的正常运行，不宜对其负荷有影响。

7.4.3 报警管理系统宜设置与MES、设备管理系统、安全管理平台等的通信接口。

7.4.4 报警管理系统应用服务器应安装多块独立的以太网网卡，分别与基本过程控制系统和MES等网络相连。

7.5 网络配置与安全

7.5.1 报警管理系统单独组网时，宜设置独立的OPC服务器和应用服务器，并采取以下网络安全措施：

a) 应用服务器与OPC服务器之间应设置硬件防火墙。防火墙宜默认设置为数据单向传输，仅允许数据从OPC服务器向应用服务器传输；若某些先进报警功能需要数据双向传输，应评估并采取必要的网络安全措施后再实施；

b) 应用服务器与MES等工厂信息网之间应设置硬件防火墙或网闸等网络安全措施。防火墙或网闸应默认设置为数据单向传输，仅允许数据从应用服务器向MES等外部系统传输；

c) 应用服务器、OPC服务器及其客户端等应采取防病毒等保护措施。

7.5.2 报警管理系统作为基本过程控制系统高级应用的组成部分联合设置时，其网络配置与安全措施应符合SH/T 3092的相关规定。

8 报警人机界面

8.1 一般规定

8.1.1 报警人机界面由报警管理系统人机界面和报警系统人机界面组成，应遵循人机界面设计的总体原则和整体规划，提高人机界面的效率和一致性。

8.1.2 报警管理系统人机界面应简洁明了，宜采用图型、文字、数字和色彩等形式展示报警概览、报警系统性能统计和报警管理信息等。

8.1.3 报警系统人机界面应符合报警原则和人机工程学的原则，有助于操作员快速确定报警位置并进行正确的报警响应操作。报警系统人机界面的设计应考虑控制系统的能力。

8.2 报警管理系统人机界面

8.2.1 报警管理系统的客户端应独立于基本过程控制系统的操作员站。

8.2.2 报警管理系统的人机界面功能宜包括报警系统性能指标统计、实时报警管理、报警指导信息、交接班日志管理、信息推送管理和其他报警管理画面。

8.2.3 报警管理系统应能按周报和月报等形式对报警系统关键性能指标（KPI）按照工艺分组、班组等进行统计、汇总并呈现。报警系统性能指标统计报表宜包括：

a）报警汇总列表；

b）频繁出现报警的报表 （如前10个频繁出现的报警）；

c）报警抑制（如手动抑制、自动抑制）报表；

d）报警停用报表；

e）滋扰报警报表；

f）与报警数据库对比报警设置差异报表。

8.2.4 报警管理系统宜具有实时报警管理功能及相应人机界面，按照预定的工作流程实施报警分析、归档记录并可将报警系统中违反报警原则的响应操作及时告知相关岗位人员，并辅助基本过程控制系统实现报警抑制、报警停用、多工况报警等功能。

8.2.5 报警管理系统应具有报警指导信息管理功能及相应人机界面。报警指导信息宜包括：

a）报警可能原因；

b）报警可能后果；

c）报警优先级；

d）报警响应操作指导。

8.2.6 报警管理系统应具有交接班日志管理功能及相应人机界面。交接班日志管理宜包括：

a）报警抑制和报警停用清单；

b）旁路的联锁清单；

c）本班内发生的重要报警清单；

d）报警变更清单。

8.2.7 在保证网络安全的前提下，报警管理系统可提供基于网络的报警信息分级推送（如电子邮箱、移动通

讯设备等）功能及相应人机界面。

8.3 报警系统人机界面

8.3.1 基本过程控制系统（如DCS）的操作站宜作为报警系统人机界面，报警显示和声响图像等功能要求应符合SH/T 3092相关规定。

8.3.2 工艺流程图画面显示宜选用素淡的颜色，不宜使用红色、黄色、橙色等醒目颜色来指示各种正常工况、设备位号以及其他非报警内容。报警显示颜色宜选用亮红、亮黄、橙色等醒目颜色，已选用的报警颜色在流程图画面中不宜再使用。高优先级的报警应比低优先级的报警颜色更为醒目，未确认的报警应比已确认的报警更醒目。

8.3.3 相同优先级的报警宜具有相同的显示颜色、符号和声响。不同优先级的报警宜具有不同的显示颜色、符号和声响。报警声响应响亮且区分度高，但又不宜对操作员造成过度干扰。中心控制室内不同生产装置的报警声响可不相同。

8.3.4 报警系统人机界面的设计应减少操作员进行报警识别、确认、评估和操作等的按键次数。发生报警时，应能从工艺流程画面直接切换至相关报警画面。

8.3.5 报警系统人机界面的监控分区应符合装置或单元的工艺操作要求，应能按照过程报警、仪表及控制系统诊断报警等分开显示与管理。

8.3.6 抖动报警或重复报警不应占用报警系统人机界面大量的显示空间。同一报警不宜分配至多个报警组。

8.3.7 硬件结构辅助操作台上的报警宜与报警系统中最高优先级的过程报警采用一致的设计原则。辅助操作台的报警和响应操作应在报警系统中记录。

9 工程设计与实施

9.1 工程设计

9.1.1 工程设计阶段应编制报警管理系统规格书，主要内容宜包括：

a）概述；

b）功能要求；

c）硬件配置；

d）软件配置；

e）网络架构及信息安全；

f）工程实施要求。

9.1.2 在报警原则的基础上还可编制报警管理系统功能设计规格书（FDS），更为详细地规定报警管理系统的各项功能要求、技术参数、管理规程等。报警管理系统功能设计规格书主要内容宜包括：

a）概述；

b）实施范围；

c）报警管理人员及责任矩阵；

d）网络配置及信息安全；

e）硬件功能设计；

f）软件功能设计；

g）报警性能指标；

h）报警辨识与合理化分析；

i）报警人机界面设计；

j）报警分类和分组设计；

k）报警优先级划分；

l）报警抑制和报警停用设计；

m）特殊报警设计；

n）工程设计与实施；

o）运行、维护与变更管理；

p）性能监测、评估与审查；

q）培训。

9.1.3 报警管理系统的工程设计应根据报警原则及功能设计规格书要求，在报警辨识和合理化分析的基础上，确定相关报警设置和人机界面，主要内容宜包括：

a）报警位号；

b）报警描述信息；

c）报警设定值；

d）报警分类；

e）报警优先级；

f）报警死区；

g）报警延迟；

h）多工况报警；

i）报警人机界面。

9.2 工程实施

9.2.1 应根据工程设计文件对报警管理系统和相应的报警系统开展集成、组态、下装、调试等工作。

9.2.2 应进行报警管理系统的工厂验收测试（FAT），宜开展报警管理系统与基本过程控制系统的工厂集成验收测试（IFAT）。

9.2.3 应开展报警管理系统的工程实施培训和操作管理培训。

10 运行、维护与变更管理

10.1 运行

10.1.1 应制定报警管理系统运行、维护与变更管理的管理规程，明确各人员岗位职责，按照已批准的管理规程开展各项报警管理工作。操作规程宜明确报警的响应操作要求和方式，并对相关岗位人员进行培训。

10.1.2 产生报警时，操作员应按照报警原则及管理规程进行正确的响应操作，阻止或延缓危险事件发生。典

型的响应操作宜包含：

a）在控制室进行操作调整；

b）现场开关阀门；

c）停用处于异常工况的设备；

d）启动备用设备；

e）启动应急预案；

f）通知相关部门开展维修工作。

10.1.3 多个报警同时发生时，应根据设定的报警优先级别先处理高级别的报警。

10.1.4 操作员发现报警设置不能适应生产需要时，应及时汇报，开展报警评估和变更管理。不应随意更改报警设置。

10.1.5 报警响应操作完成后，应记录报警处置过程，并分析报警原因。对当班未解决的报警事件应记录和交班。

10.1.6 管理人员应定期检查报警及其处置情况的记录，将报警泛滥事件及时告知相关工艺、设备、仪表、电气等部门及人员，按需要开展原因分析工作，制定有针对性的报警改进措施并组织落实。

10.2 维护

10.2.1 报警管理系统应按照报警原则及管理规程定期进行测试与维护，保存测试和维护记录。若测试发现报警设置、报警系统和报警管理系统存在问题，应尽快开展维修维护工作。

10.2.2 与安全仪表系统相关的报警应按照管理规程开展周期性测试，并对测试结果进行记录。

10.2.3 应通过报警管理系统的负责人员开展系统维护工作，保持报警管理系统的完整性和有效性。

10.3 变更管理

10.3.1 为保证报警管理系统的完整性和有效性，应建立报警变更管理（MOC）的工作流程和管理规程，有效地管理报警变更工作。报警变更管理宜经过申请、评估、审查、批准、实施、培训、监督等流程。

10.3.2 报警变更管理宜包括如下内容：

a）创建新报警；

b）删除现有报警；

c）更改报警优先级；

d）更改报警设定值；

e）更改报警类型；

f）更改报警描述信息；

g）更改HMI操作画面中报警显示；

h）添加、修改、更新报警抑制、报警停用或多工况报警设置方案。

10.3.3 变更审批通过并实施后，报警管理系统的的报警数据库应同步更新。

11 性能监测、评估与审查

11.1 报警性能监测

11.1.1 报警管理系统应对报警系统关键性能指标（KPI）进行实时监测，持续发现报警问题并采取纠正措施。

11.1.2 报警性能监测的主要量化报表或报告宜包括：

a）报警系统关键性能指标统计报表；

b）频繁出现报警的报表（如前10个频繁出现的报警）；

c）抖动报警列表和数量；

d）陈旧报警列表和数量；

e）报警泛滥的时间百分比；

f）报警抑制列表及持续时间；

g）报警停用列表及持续时间；

h）HSE报警列表和数量；

i）仪表及控制系统诊断报警列表和数量；

j）报警响应操作事件报表。

11.1.3 报警管理系统应按管理规程定期（如每周、每月）发布各项报警性能监测报表或报告给相关岗位人员。

11.2 报警性能评估

11.2.1 应定期（如每月、每季度等）对报警性能监测结果进行评估，及时发现报警设置、报警系统和报警管理系统存在的问题。

11.2.2 对报警性能评估发现的问题应制定合理的解决提升方案，并组织落实，持续改进报警性能。

11.3 审查

11.3.1 在报警管理生命周期内，应定期（如每年）组织开展报警管理系统的审查，发现在报警性能监测与评估过程中未发现的问题和需改进提升之处。

11.3.2 审查需要准备的资料宜包括：

a）报警原则；

b）报警数据库/报警台账；

c）报警性能监测与评估报告；

d）报警相关的变更；

e）报警系统和报警管理系统的测试记录；

f）操作员的培训记录；

g）相关事故调查报告等。

11.3.2 审查内容宜包括：

a）报警设置的合理性；

b）报警系统设置的报警参数与报警数据库的一致性；

c）报警优先级设置的合理性；

d）报警响应操作时间是否充足；

e）报警设置的相关变更记录；

f）报警性能监测与评估报告的改进；

g）无效报警是否得到有效解决；

h）报警管理系统的岗位及其职责分工是否清晰明确；

i）报警抑制和报警停用是否经过审批；

j）报警响应操作程序是否培训。

11.3.3 应根据审查结果制定整改计划并组织实施，进行持续的改进提升。

附 录 A

（资料性附录）

报警系统关键性能指标（KPI）

报警系统的关键性能指标（KPI）可基于每个操作岗位至少30天的数据，典型的报警关键性能指标如表A所示。

表A 报警系统关键性能指标（KPI）（基于每个操作岗位至少30天的数据）

KPI指标	目标值[a]	
	可接受的	最大可控的
每天报出的报警数	小于144个	小于288个
每小时报出的报警数	平均小于6个	平均小于12个
每10 min报出的报警数	平均小于1个	平均小于2个
每小时超过30个报警的时间百分比	小于1%	
每10 min超过10个报警的时间百分比	小于1%	
在10 min内报警的最大数量	不大于10	
报警泛滥的时间百分比	小于1%	
前10个频繁出现的报警占所有报警的百分比	1%~5%	
抖动报警和瞬时报警的数量	零	
每天报出的陈旧报警数量	少于5个	
各优先级的报警所占比例[b]	第一级（紧急）过程报警约占5% 第二级（重要）过程报警约占15% 第三级（一般）过程报警约占80%	
未经审批的报警抑制和报警停用	零	
不合理的报警设定值修改	零	

注：a) 表中供参考的报警关键性能指标是根据石油化工工厂或装置多年经验及相关国际、国内规范提出的目标，超出这些报警KPI指标通常意味着操作员面对的报警负荷过重，针对报警的响应操作效率降低，并可能产生安全隐患，需予以改进。不同石油化工工厂或装置的报警系统关键性能指标（KPI）根据各自工艺特点和操作员的水平不同而各异，可按照实际评估结果确定。

b) 仪表及控制系统诊断报警不计算占比，分开显示汇总。

附 录 B

（资料性附录）

报警优先级划分评估典型工作流程

报警优先级划分评估典型工作流程见图B。

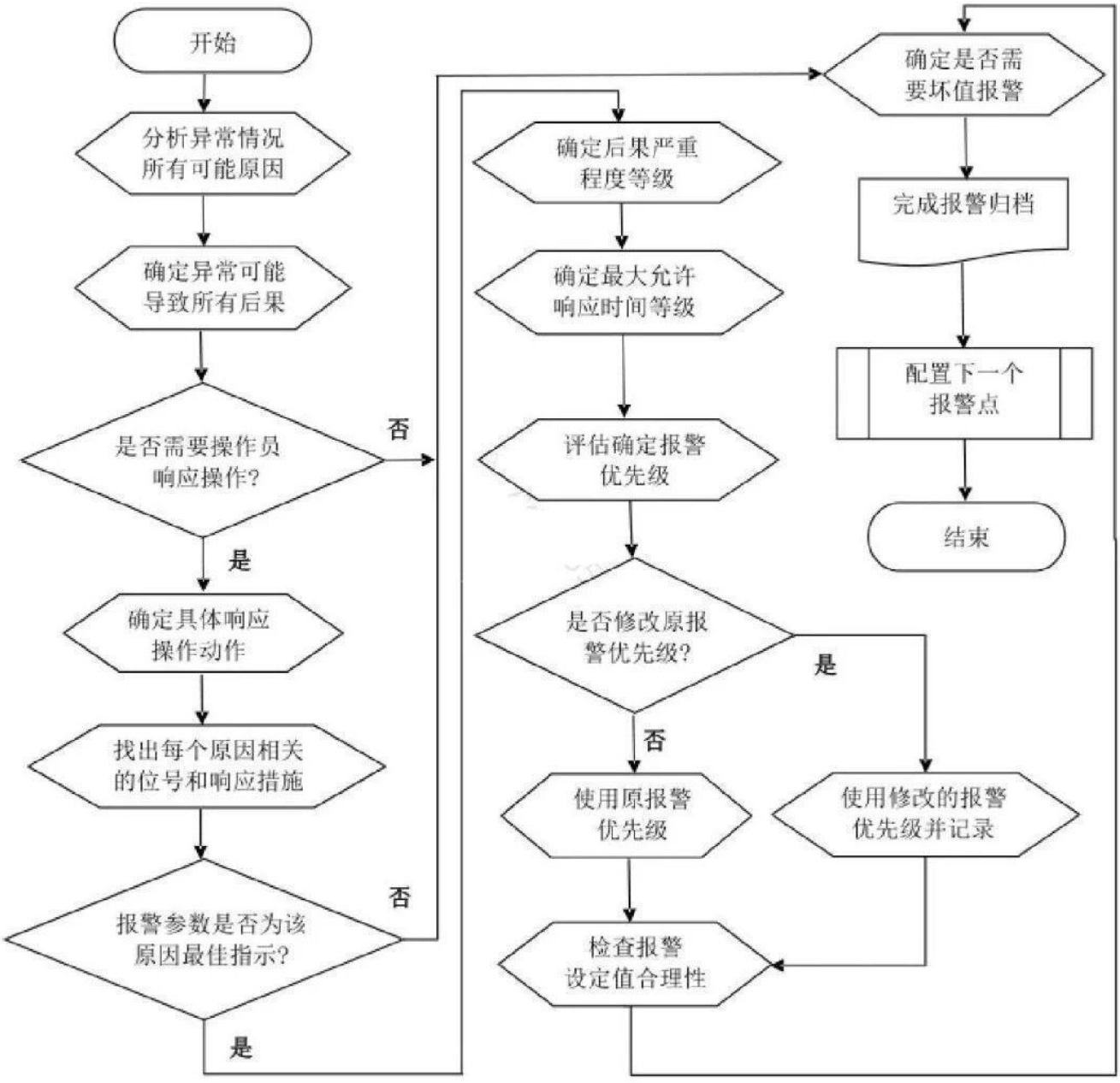

图 B 报警优先级划分评估典型工作流程