基于风险分析的报警管理

鲁毅[1] 刘昳蓉[2] 袁小军[2] 冯双虎[2]

北京华清国诚安全技术有限公司

摘要：危险与可操作性研究（HAZOP）是一种定性的风险分析方法，用于辨识设计缺陷、工艺危害及操作性问题的结构化、系统化分析方法。考虑到 HAZOP 分析过程中关于后果及现有措施分析时存在量化不足等局限性因素，因此本文引进报警管理理念，通过 HAZOP 与报警管理的有效结合，可在设计阶段基于 HAZOP 分析的原因后果，对现有措施中报警进行半定量评估以确定其不同的优先级，同样对在役装置的报警系统进行诊断分析，评估报警有效性，识别现有报警系统的不足，提出针对性的方案，可避免因此而带来的经济损失。

本文通过对国内外发生的多种化工事故的原因分析，指出产生事故均与报警管理的缺陷有关，不完善的报警管理可能导致不必要的停车，降低了装置的平稳安全运行的能力。本文以国内某变换装置为例，分析了基于 HAZOP 分析的报警管理在设计阶段及在役阶段等不同阶段的应用，并举例说明了报警分级及 KPI 指标评估的具体方法。

关键词：HAZOP；报警管理；报警分级；KPI 指标

Alarm Management based on Risk Analysis

Lu Yi[1], Liu Yirong[2], Yuan Xiaojun[2], Feng Shuanghu[2]

(Industry Risk Control, Beijing, 100025, China)

Abstract: HAZOP is a qualitative method used to systematically identify hazards in the design and operation phase of a plant. Considering the limitation that HAZOP consequence and safeguard are difficult to further quantitative analysis, the alarm management principle will be introduced in the articles as follows. By using the method from alarm management, the process alarms as HAZOP safeguard can be classified to several different level according to the severity of scenario consequence and response time. For the operating plant, the alarm system can be optimized by analyzing KPI indicators to avoid the safety risk occurrence and property loss due to shutdown and restart of plant.

Base on analysis consequence of chemical accidents, the conclusion is that design defects and deficiencies of alarm management has become one of the main causes. Incomplete alarm management can lead to unplanned plant shutdown and reduce performance of the plant operation.

To takes certain CO transformation plant for example, the application method of alarm management based on Risk analysis was further analyzed during the design and operating phases, and the methods of alarm classification and KPI indicator assessment are also explained.

Key words: HAZOP; Alarm Management; Alarm Classification; KPI

引言

随着我国对能源及化工品需求的高速增长，石油化工及煤化工联合装置在保障我国能源安全的政策引导下，近年来得到大力扶持和发展。装置规模的大型化、工艺流程复杂化，操作自动化等要求，给装置的稳定安全运行及人员安全带来了前所未有的挑战。

因此我国在相关的法律法规上加强了重视，如中国国家安监总局根据国际电工委员会发布的 IEC61882:2001HAZOP 实施导则，翻译并转化成（AQ/T3049-2013）《危险与可操作性分析（HAZOP）应用导则》并先后发布 76 号文和 88 号文，要求凡是涉及“两重点一重大”的新建装置必须在基础设计阶段展开 HAZOP 分析，在役装置要采用 HAZOP 分析方法，一般 3~5 年一次。

但是在报警管理上，目前国内没有相关的法律法规，在装置在设计阶段也没有完整的报警管理程序，同时随着近年 DCS 系统的迅速发展，报警组态变得非常容易，人们可以在不增加成本的基础上随意设置报警，因此“报警越多越好”以及“组态不花钱”等因素主导了人们的主要思想，从而忽略了报警管理重要性。具统计目前工艺装置中单个 PID 回路通常有 15-20 个报警，包括高低报警、偏差报警、速率报警等，这些报警的数量繁多，有时甚至比工艺参数报警更多。

由于当前的 HAZOP 分析往往存在点到为止的现象，对报警的增加或者删除往往只是根据人员的经验进行主观判断，缺少必要的依据。目前报警的分级的现状是仅依靠系统供应商根据工程经验进行设置。以某 ITCC 集成商为例，系统中 90%的报警默认为高优先级报警，报警指示灯及声音始终处于活跃状态，极大的牵扯了操作人员的精力。经过长时间的运行，操作人员往往已经习惯这种反复无常的报警，所以当报警发生时，操作人员往往会直接进行报警确认，因此则可能忽略了重要的安全隐患。

随着近年来各类事故的不断发生，更多的化工企业开始加强对重视报警管理的重视程度。如何能够在风险分析的基础上实现报警的功能是目前所遇见的典型问题。本文将从设计阶段及运行阶段两方面对基于风险分析的报警管理进行论述。

1 技术简介

1.1 风险分析

目前风险分析的方法有多种，如 HAZOP、Hazard、PHA、What-If 等，HAZOP 作为一种系统化、结构化的危害识别工具已经广泛用于识别装置在设计和操作阶段的工艺危害。HAZOP 分析由一组多专业背景的人员，以会议的形式，将装置划分为若干小的节点，使用一系列的参数和引导词构建偏差，采用头脑风暴的方式对工艺过程中危险和可操作性的问题进行分析研究。它是一个程序化的、正式的、系统的审查过程，可以评估装置潜在的设计失误或误操作，以及其对整个装置运行的影响。

HAZOP 分析将不同工艺过程划分为适当的节点，采用引导词引导的方法，尽量找出偏离设计意图的所有可能的偏差。下述关键分析过程应给予特别关注。

划分节点

每张 P&ID 上节点的划分，应保证 HAZOP 审查详细、全面、有效。节点可以是流程中的一段管线或一个设备或其组合。在分析每张 P&ID 时，为保证分析效果，分析小组每次应仅重点讨论一个关注点。节点应在 P&ID 上进行采用不同颜色明确标识，说明每个节点的编号、起止点和中间部分，若一个节点涉及多张 P&ID，节点标识还应包括 P&ID 的连接编号。

解释设计意图

工艺工程师有责任向分析小组成员解释所分析的流程或节点的设计意图。只有分析小

组成员对设计意图和参数有了清楚准确的理解和把握，才能保证之后 HAZOP 分析的讨论富有成效。

偏差

分析每个节点时，都应将引导词与适当的工艺参数组合，以生成偏离了设计意图的偏差。例如“无”这个引导词通常和“流量”组合在一起，表示“无流量”这个偏离，其他引导词“过大”、“反向”“过小”等和“流量”组合在一起，则表示“流量过高”、“逆流”、“流量过低”等偏差。

评估后果和安全措施

对每个有意义的偏差，分析小组都应对所有直接和间接的后果进行分析评价。另外，对那些在设计中已有的、可以防止危险发生或减轻其后果的安全措施，也应进行讨论、记录。在分析后果时如果还需要其他额外信息，则应将该情况作为对将来下一步工作的要求，记录在分析报告中，然后继续 HAZOP 分析。建议由 HAZOP 分析主席指派收集信息的负责人。应尽量在 HAZOP 分析会议上解决尽可能多的关键问题、难题。

风险分类

在 HAZOP 分析中对每个偏差所导致的风险进行风险分类的目的，是帮助定性评估偏差风险程度，并由此确定分析结论中每项建议措施的优先级别。

结论记录和建议措施

HAZOP 分析记录表应记录所有有意义的偏差。在讨论这些偏差时，HAZOP 分析秘书应记录与会者达成共识、取得一致意见的所有信息。每个偏差讨论时至少应该记录引导词、偏差、原因、后果、风险类别、安全措施（若有）、建议措施（若有）、责任方。在每天 HAZOP 分析会议结束后，应由秘书向与会者提供当天的 HAZOP 分析清单供其审阅。

HAZOP 分析流程大致上是一致的，具体流程见下图：

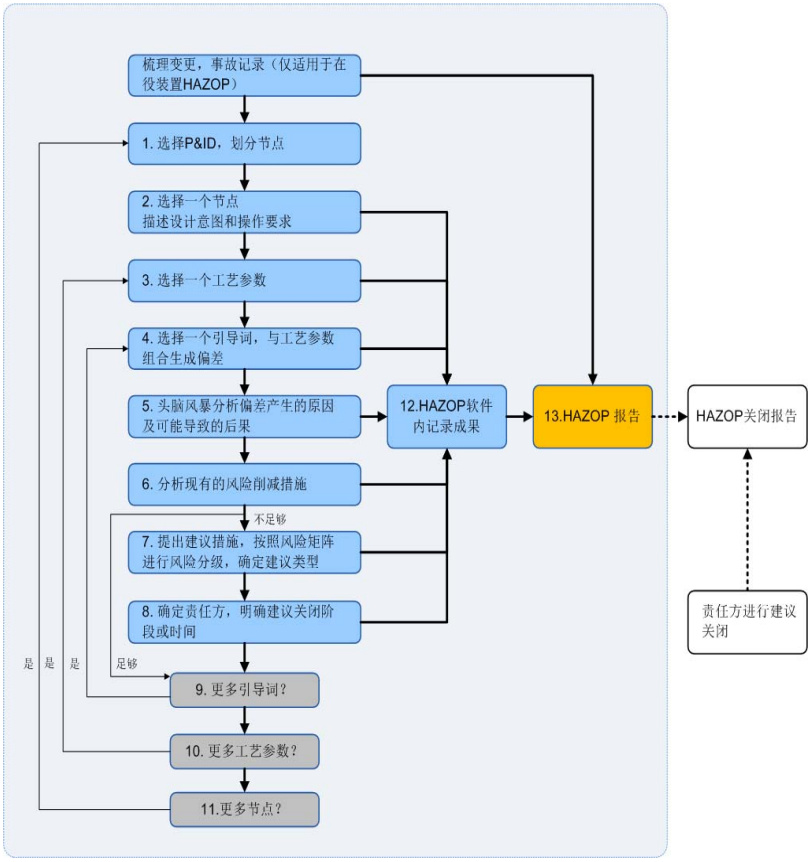

图 1 HAZOP 分析步骤

Fig.1　HAZOP Procedure

1.2　报警管理

报警就是采用声光等手段提醒控制室操作人员对工艺装置采取有效的行动。可以通过各种措施来消除报警，恢复平稳操作，如调整工艺参数、通过对讲机通知外操调节操作、查询仪表读数、停启设备等。设置有效的报警，能够良好的反应装置的运行状态，操作人员采取正确的处理手段，能够使装置平稳安全长周期的运行下去。报警作为关键的预防风险发生的手段，是保护层中非常关键的一环，如下图所示。

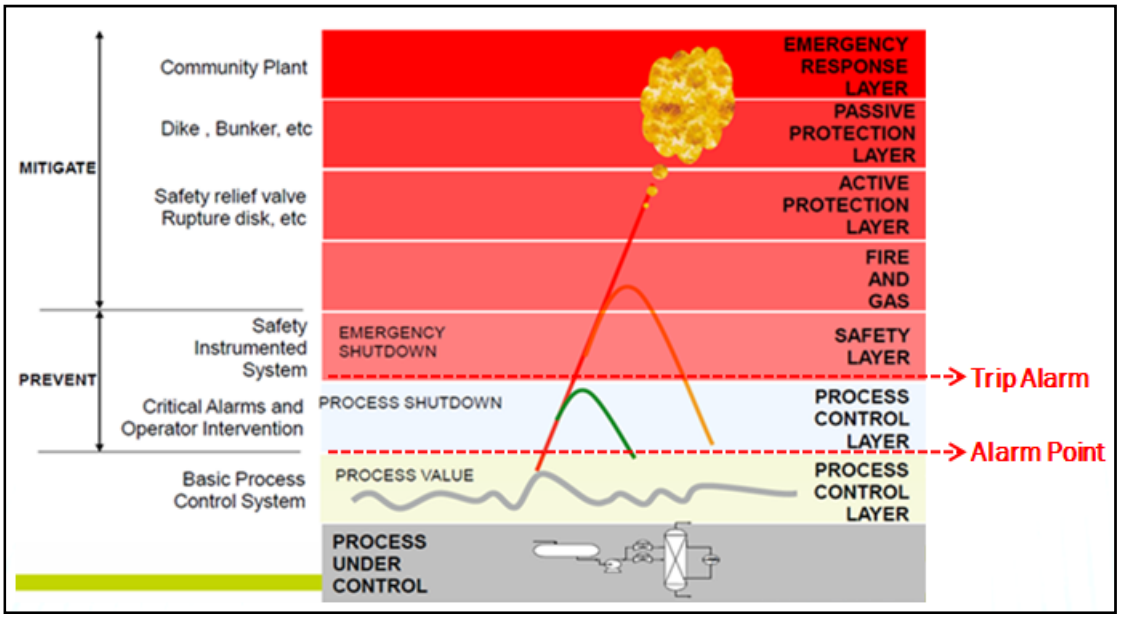

图 2　保护层

Fig.2　Protection layer

报警管理是通过制定完整有效的报警设计流程和管理策略，或改善现有装置中已有的报警管理体系，来避免更大的财产损失以及环境、安全事故的一种手段。报警系统是协助操作人员发现工艺、设备或系统问题并优先作出响应，防止发生不可控的后果。同时为其他分析人员采集离线信息，方便后期的维修工作及事故的调查工作。但报警不是万能的，它并不能够取代操作人员对装置的操作和监控。

本文通过介绍国内石油化工行业在报警管理方面存在的主要问题，说明报警管理的有效性及必要性。并且提出化工装置应当在设计阶段及操作阶段等不同阶段的执行要点，并举例说明了报警评估及诊断的方法。下图为报警管理的流程图：

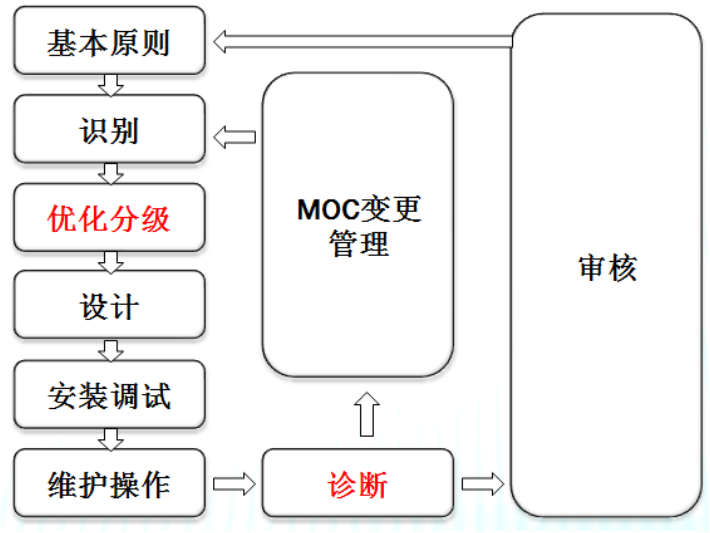

图 3 报警管理生命周期

Fig.3 Alarm Management Lifecycle

1.2.1 报警评估（分级）

KPI 指标

无论设计阶段还是运行阶段，KPI 指标均为评估报警系统有效性的重要手段。设计阶段 KPI 指标（EEMUA191）如下图所示：

表 1 KPI 指标（设计阶段）

Table 1 KPI （design phase）

Priority band	Alarms configured during system design
Critical	About 20 altogether
High	5%
Medium	15%
Low	80%

运行阶段的 KPI 指标（EEMUA191）如下表所示：

表 2 KPI 指标（在役阶段）

Table 2 KPI （operation phase）

Priority band	Target maximum occurrence rate
Critical	Very infrequently
High	5 per shift
Medium	2 per hour
Low	5 per hour

报警矩阵

国际标准中，EEMUA191、ISA18.2 以及 SCADA1167 分别制定了不同的报警优先级评估方法。本文以 SCADA1167 风险矩阵法为例，对报警优先级划分进行阐述。首先，需要评估出每一个报警回路的后果严重性等级和相应时间，参见表 3 和表 4。

表 3 后果严重性

Table 3Severity of consequence

Impact	Category	Severity: MINOR	Severity: MAJOR	Severity: SEVERE
Personnel Safety	No injury or health effect	Personnel injuries	1 death	More than 1 death
Public or Environmental	No effect	Operating permit levels or other mandates not exceeded Local environmental effect not crossing fence line or right-ofway, no community complaints Contained release with little, if any, clean up and negligible financial consequences Internal or routine reporting requirements only	Operating permit levels exceeded to a degree involving local or state reporting Single exceedance of statutory or prescribed Limit Contamination causes some non-permanent damage Single or very few community complaints expected Reporting required a the local or state agency level	Operating permit levels exceeded to a degree involving federal reporting Limited or extensive release, crosses fence line or right-of-way Impact involving the community, multiple complaints expected Repeated exceedances of limits Uncontained release of hazardous materials with environmental and third party impact Extensive cleanup measures or financial consequences
Cost / Financial Loss / Down-time	No loss	Event costing <$10,000. Only internal reporting required. No pipeline outage or delivery impact	Event costing $10,000 to $100,000 Reporting required at the regional level Short duration outage; daily throughput not significantly affected	Event costing >$100,000 Reporting required at senior management level Pipeline outage; customer deliveries and/or schedule affected

表 4 响应时间

Table 4 Response time

Classes for maximum time to respond	
Response time introduction	**Response time**
Immediately	>5minutes
Rapidly	5-15 minutes
Promptly	15-30 minutes
Upper Limit	>30 minutes

其中，HAZOP 分析出来的危险场景及相应的后果严重性可以作为报警等级划分的输入，可以作为支撑报警管理的一项重要内容。具体的分级方法可以参见表 5。

表 5 报警矩阵（SCADA 1167）

Table 5　Alarm matrix（SCADA 1167）

Maximum time to respond	Alarm consequence severity		
	Minor	Medium	Severe
>30 minutes	cancel	No need	reconfiguration
15~30 minutes	small	samll	medium
5~15 minutes	samll	medium	medium
>5 minutes	medium	high	high

Note：Risk severity need consider combine all the safety, environment and asset consequence.

响应时间通常是指操作人员从发现报警到处理正常所必须花费的时间。由此可见，如果一组报警值与其相对应的联锁值设置不当的话（如，一个液位低报警至液位低低报警的时间只有 5 分钟，实际需要 15 分钟才能恢复正常操作），那么这样的报警值就是无效且不必要的。因此在设计阶段需要对报警值和联锁值的确定投入更多的精力，即提高对 HAZOP 分析等一些分析方法的重视程度，保证报警值设置有着充足的响应时间，这样才能在运行过程中降低各种非计划停车的次数和概率。

1.2.2　报警诊断

设计阶段主要侧重对报警优先级的设置，在运行阶段则主要对现有报警系统产生的数据进行分析，从而有效的发挥报警的功能，并保证装置的长周期运行，分析过程如下所示：

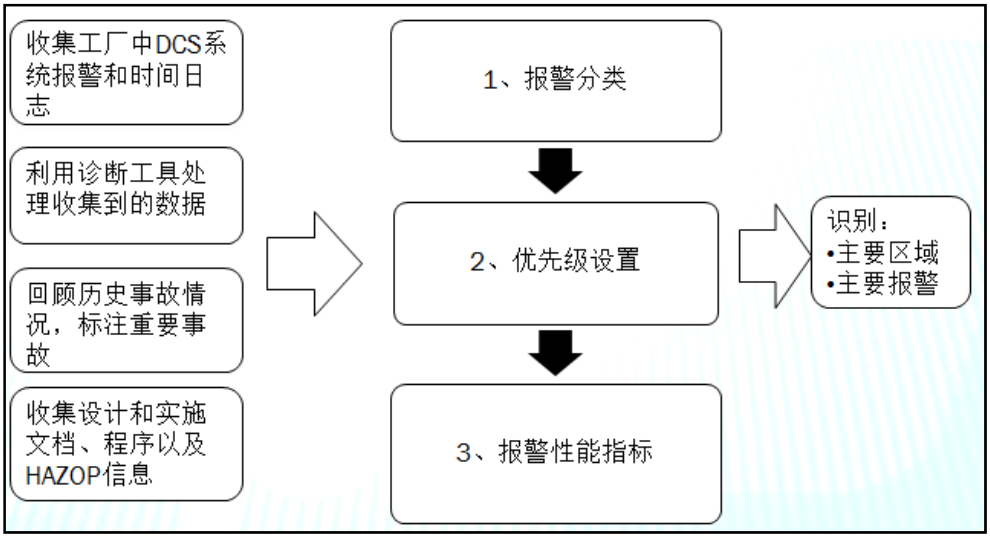

图 4 在役阶段报警管理流程

Fig.4　Alarm management process in operation phase

在装置正常运行过程中出现的报警一定是有问题的。它可能是报警设置的不当、仪表故障、或者是出现异常工况等。因此，无论报警的真假而或报警设置的不合理，均需要管理人员和操作人员对出现的每一个报警进行关注。

1)　报警数据收集

在役装置对报警进行优化管理，首先要对报警数据进行收集，具体的内容如下：

- 收集工厂中 DCS 系统报警和时间日志；
- 利用诊断工具处理收集到的数据；

- 回顾历史事故情况，标注重要事故；
- 收集设计和实施文档、程序以及 HAZOP 信息。

收集完成这些数据之后，需要管理人员和技术人员对其进行系统的分析和梳理并完成归档，把报警分为：

- 常驻报警数量；
- 厌烦报警数量；
- 无响应报警数量；
- 停用的报警。

同时分析归纳同类报警的报警频率，列出报警的平均报警率，列出优先级设置不合理的报警，辨识出特定时间段或区域严重等级，对这些不合理的报警，管理人员组织人员对报警进行合理化改进，对报警进行变更，使其使用与目前的装置运行。

2) 报警优化

步骤一：找出不合理的报警之后，需要对这些报警值进行优化变更。针对不同级别的报警值变更，需要技术人员和管理人员投入不同的关注度，但是均需要仔细讨论变更前后的工艺参数变化，识别出场景可能发生的危险，判断出变更后可能产生的后果，找出正确快速处理报警的办法。使变更后的报警更加合理有效。去除和新加的报警比之变更的报警需要更为慎重的处置方式。

步骤二：将这些不合理的报警进行进一步的归类，确立报警性能指标，参见表 6。

表 6 报警性能

Table 6 Alarm performance

Average of alarm rate (steady operation)	Acceptable level
1 per minute	Unacceptable
1 per 2minutes	Over load
1 per 5 minutes	Controllable
<1 per 10 minutes	Easily accept

装置正常运行过程中出现了报警，需要对该报警进行仔细的记录和分析。记录中的内容应包括：报警的具体位号和位置，报警时间，分析报警原因，处理方法，恢复至正常操作的时间。还可以进一步扩展得出，如何避免该报警的发生，是否有类似的报警等内容。每天汇总各个班组的报警记录，将报警按表 4 的方式进行分类，以每 1~2 周为一个周期，管理人员、技术人员和操作人员一起对超载和不能接受的报警进行进一步的处理和优化变更。从而提高报警的有效性和必要性，使装置平稳安全长周期的运行。

每天各个班组的记录汇总之后，制成饼图、平均报警率、最大报警率、TOP10 报警等等，对全年装置报警优化成果进行分析，方便存档、年度总结和制定未来的运行和管理计划。

3) 加强人员技能培训

无论设置多么可靠的报警、多么精良的设备和良好的安装，如果操作人员的操作水平不能满足要求，突发情况的处理手段不到位，紧急事故状态下的应急响应不清楚。那么再好的装置、再准确的报警、再充足的响应时间也无法保证装置平稳安全的运行。

如今装置的自动化程度很高，工艺参数、报警和联锁多达几百上千个，对操作人员的技

能水平提出了更高的要求。因此，不仅需要加强员工普通的操作技能水平，还需要进一步加强人员对报警及联锁时的响应即异常工况的处置。

应急演练的仿真度高低和演练方案的好坏决定了一次应急演练的效果，重视每一次的演练，才能让员工在真正发生突发状况时，能够做出最正确的应对，降低事故发生的后果，减少不必要的损失，使装置能够平稳安全长周期的运行。

1.2.3 人机界面优化

通过每一个风险场景的响应时间和风险严重性等级，我们能够将每一个报警进行分级。对分级过后的报警进行管理，从人机界面的角度，有如下方法：

- 针对不同级别的报警，我们可以用报警颜色来加以区别（如，红、黄、绿），便于操作人员在众多报警中，准确且及时的处理紧迫性较高的风险，从而稳定装置的运行；
- 对于不同级别的报警，我们可以在报警声音上加以区别；
- 不同级别的报警复位要设置不一样的要求，对紧急性高的报警，要提高复位的要求，防止操作人员麻痹大意，对报警进行了复位而未进行操作上的调整，可以通过增加确认对话框等手段来实现。

2 案例分析

2.1 报警优化分级

本文以某化工装置耐硫变换单元中第一变换反应器的 HAZOP 分析及报警优化为例，对变换反应器出口温度 TAH2003 为例，采用报警矩阵法进行分级。变换反应器 PID 图如下所示：

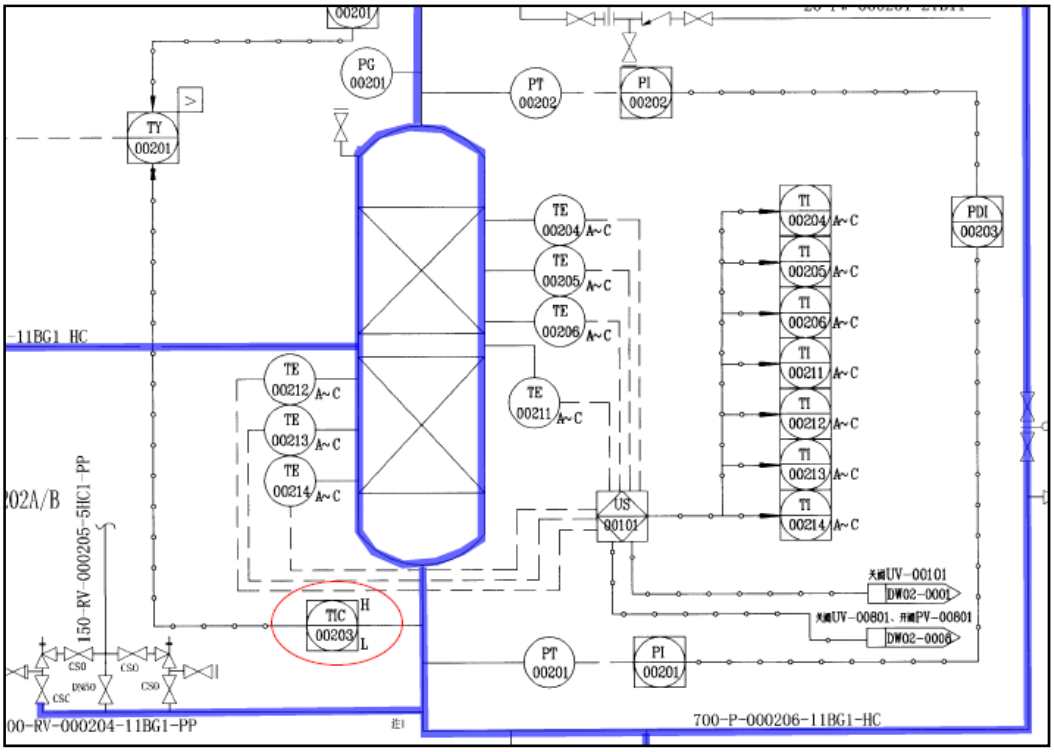

图 5　第一变换反应器 PID 图

Fig.5　Alarm management process in operation phase

对变换反应器的进行 HAZOP 分析后，导致变换反应器超温的原因为：进合成气分液罐 721-D101 原料气流量过低或无流量、进变换反应器 721-R-101 原料气温度过高，分析工作表如下：

序号	参数	偏差	偏差描述	原因/关注	后果	现有措施	S	L	R	建议措施	建议类别	建议号	责任方	备注
1.6.2	温度	温度过高	1.6.2 进变换反应器721-R-101原料气温度过高	TIC-00201/TIC-00203高选控制回路故障（TV-00201A/B开度过小或关闭）	变换反应器721-R-101床层温度升高，催化剂活性受影响，可能飞温。	原料气预热器721-E-101出口管线TI-00209；HC-00201；第一变换炉床层温度TSHH（3oo21）联锁触发US-00101	4	3	H	确认联锁高压蒸气管网设置，确保变换单元停车时蒸气量可满足安全停车要求。	S	#1.11	SEI	72100PE-DW02-0002
1.2.1	流量	流量过低或无流量	1.2.1 进合成气分液罐721-D101原料气流量过低或无流量	上游单台气化炉跳车	变换系统压力降低，第一变换炉721-R-101出口温度升高，可能超温。	气化来原料气管线上FIQ-00101、PI-00101；第一变换炉出口TIC-00203带TAH；第一变换炉床层温度TSHH（3oo21）联锁触发US-00101								

图 6 HAZOP 分析表格

Fig.6 HAZOP Worksheet

从上述分析结果可以看出，TAH2003 在第二条原因中可作为保护措施，但是其有效性及必要性没有进一步分析。下面采用报警矩阵法对 TAH2003 作进一步的分析，以确定以优先级。

本次报警分级采用 SCADA1167 报警矩阵，报警矩阵如下所示：

表 7 报警矩阵

Table 7 Alarm matrix

Maximum time to respond	Alarm consequence severity		
	Minor	Medium	Severe
>30 minutes	cancel	No need	reconfiguration
15~30 minutes	small	samll	medium
5~15 minutes	samll	medium	medium
>5 minutes	medium	high	high

Note: refer to table 3 and 4 to confirm consequence and response tim

报警分级过程需结合 HAZOP 分析的成果，列出导致报警的所有原因，根据各原因中后果严重性及相应时间确定报警优先级，具体的工作表如下图所示：

序号	位号	原因	后果	保护场景	设定点	物理边界点	变化速率	响应时间	操作时间	修正	S（后果严重性）	T（时间紧迫性）	Alarm等级
1	TAH 00203	进合成气分液罐721-D101原料气流量过低或无流量	变换系统压力降低，第一变换炉721-R-101出口温度可能升高。	变换反应器超温	425	475	10	5			中	低	低
		进变换反应器721-R-101原料气温度过高	变换反应器721-R-101床层温度升高，催化剂活性受影响，可能飞温。	变换反应器飞温	425	475	20	2.5			大	中	中

图 7 报警分级工作表

Fig.7 Alarm classification worksheet

由于 HAZOP 阶段，报警一览表尚未完善，因此报警设定点无法确定。通过查询“工艺说明书”，确定正常操作温度为 400℃，此处假设报警值为 425℃。通过查询“设备数据表”，得出物理边界点为 475℃。

由 HAZOP 分析结果可以看出，导致第一反应器温度高报警 TAH00203 的原因分别：（1）合成气分液罐 721-D101 原料气流量过低或无流量；（2）进变换反应器 721-R-101 原料气温度过高。原因（1）导致的后果为变换系统压力降低，变换反应器出口温度可能升高，由此判断其后果严重性为“中”。假设温升为 10℃/Min，则其响应时间为 5Min，综合判断报警

优先级为“低优先级”。同理，原因（2）由于其后果存在反应器飞温场景，所以其后果严重性为“大”。假设温升为 20℃/Min，其响应时间为 2.5Min，则其报警优先级为“高优先级”。综合考虑两个原因，其优先级为“高优先级”。根据 SCADA1167 标准要求，“高优先级”报警应配置为高频率声光报警。

按上述方法可对装置内所有报警进行定级，同时还需考虑 KPI 指标的影响，以控制报警数量在合理可接受的范围。

2.2 报警诊断

本文通过对某酸性气处理装置采用 ALRSuite 软件进行了报警诊断分析，该装置为分析前每小时报警数量为 120-125 条/小时，根据 EEMUA191 的标准最小的标准为 1 条/分钟，由此可以看出本装置报警系统处理泛滥的状态（不可接受状态）。工作组按“1.2.2 报警诊断”的工作流程进行分析，不同阶段报警数量，如下图所示：

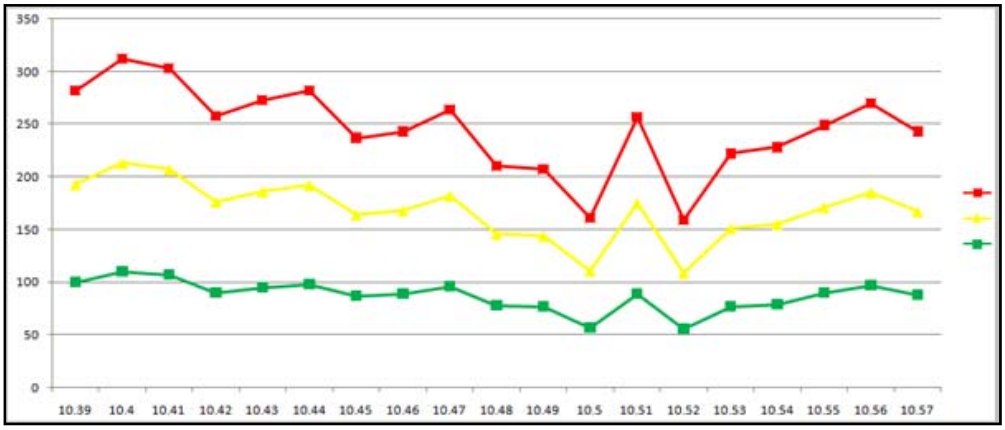

图 8 报警趋势图

Fig.8 Alarm Trend Diagram

通过对该装置为期 5 个月的分析，平均报警率削减我 12 条/小时，重复报警及无效报警削减了接近 90%，大大的提高了报警有效性及操作人员的效率。

3 结论

HAZOP 分析与报警管理的有效结合极大提高了风险分析的科学性及准确性，本文以实际装置为例，分别从设计阶段、在役阶段对基于风险分析的报警管理进行了论述，并总结了一整套分析发方法，以促进基于风险的报警管理工作的顺利进行。

安监总管三[2014]116 号-《国家安全监管总局关于加强化工安全仪表系统管理的指导意见》重点强调了报警管理的重要性，并规定了安全仪表功能完整性相关的报警参照安全仪表功能进行管理和检验测试。因此制定一套完整的报警生命周期管理程序已经迫在眉睫。报警的有效性和必要性及报警管理是化工行业一个任重而道远的工程，需要上至企业决策者，下至普通员工共同的努力，才能使装置得以平稳安全长周期的运行。

References

[1]. APIRP1167Pipeline SCADA Alarm Management

[2]. EEMUA191-2007Alarm Systems

[3]. ISA18.2Expected Re-Issue

[4]. IEC-61508Functional safety of electrical/electronic/programmable electronic safety-related systems

[5]. GBT20438.4-2006Functional safety of electrical/ electronic/ programmable electronic safety-related systems

[6]. ISA-84.00.01-2004Part1(IEC61511-1Mod)FunctionalSafety:SafetyInstrumentedSystemsfortheProcessIndust

rySector
[7]. ISA S88.01Batch Control
[8]. IEC 62682:2014 Management of alarm systems for the process industries
[9]. Norwegian petroleum directorate 2011 YA-711 Principles for alarm system design
[10]. EPRI 2008 Alarm Management and Annunciator Applications Guidelines
[11]. PAS 2010 The Alarm Management Handbook