ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41394—2022

爆炸危险化学品储罐防溢系统功能安全要求

Functional safety requirements of overfill prevention systems on explosive dangerous chemical

2022-04-15 发布　　2022-11-01 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。

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、丹东通博电器(集团)有限公司、中国石油集团安全环保技术研究院有限公司、中国石油天然气管道工程有限公司、南京理工大学、霍尼韦尔(中国)有限公司。

本文件主要起草人：刘瑶、帅冰、吕东风、卜志军、张一丁、史学玲、朱明露、魏振强、李祖军、郭永刚、徐德腾、陈小华、张占峰、陶明、钱福群、魏海洋、施隋靖、于世恒、王璐、杨柳、李秋娟、孙腾、陈红新、钱华、朱旭营、王刚、张亚彬、段栋德、刘晶晶、王荣臻、刘文才、熊文泽。

引　言

在石油库区、化工园区及危险化学品相关运营单位，危险化学品储罐是重大危险源，一旦发生溢流，可能导致火灾爆炸进而引发重大人员伤亡和经济损失，风险极高，储罐防溢系统是降低爆炸危险化学品储罐溢流风险的必要手段，为保障人民群众生命和财产安全，对储罐防溢系统实现全生命周期功能安全保障，具有重要意义。

本文件针对爆炸危险化学品储罐防溢系统全生命周期安全管理、风险评估、安全要求分配、设计、安装、试运行、评估、验收、维护及停用活动提出安全相关要求和技术方法，为储罐防溢系统全生命周期各阶段参与人员提供工作依据，提升我国危险化学品存储环节风险管控能力和本质安全水平。

本文件目的在于指导和规范石油及危险化学品相关领域固定式石油及其他危险化学品液体储罐防溢系统的全生命周期功能安全活动。

爆炸危险化学品储罐防溢系统功能安全要求

1 范围

本文件规定了对危险化学品储罐设置储罐防溢系统的功能安全要求。

本文件适用于5 m^3 以上的地上固定式石油及其他危险化学品液体常压储罐。5 m^3 及以下固定式液体常压储罐可参照执行。

本文件不适用于LPG/LNG罐、专用的缓冲罐、发动机燃料油罐、供暖油罐、收油仅来自于轮式的槽车(比如油罐车或铁路油罐车)的油罐。

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文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 20438.2—2017 电气/电子/可编程电子安全相关系统的功能安全 第2部分:电气/电子/可编程电子安全相关系统的要求

GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求

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

GB/T 29639 生产经营单位生产安全事故应急预案编制导则

GB 50093 自动化仪表工程施工及质量验收规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

报警 alarm

通过声音和/或可视的方式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。

3.2

警示 alert

当操作员预定义的操作条件已经达到某个值时,采用声和/或光提示操作员的方法。

注:警示的目的是提醒用户/操作员需要进行调查或者执行其他对应的动作。

3.3

常压储罐 atmospheric tank

设计压力小于0.1 MPa、建造在地面上、储存非人工制冷、非剧毒性的石油、化工等液体介质的储罐。

3.4

关注液位 level of concern:LOC

业主或操作员通过计算储罐的介质液位设置的合适的警示液位、报警液位和储罐自动防溢功能触发液位。

3.5

最高工作液位 maximum working level:MW

正常操作时储罐进料允许达到的最高液位。

3.6

极限液位 critical high level:CH

储罐进料能够达到的、无有害影响的最高液位,超过此液位即发生介质溢出或储罐损坏等情况。

注:在工程设计中,极限液位也称"储罐设计液位"。

3.7

高高液位 high-high tank level:HH

在达到极限液位(CH)之前能够终止进料或介质转运,足够低于极限液位(CH)的液位。

3.8

高高液位报警 high-high tank level alarm:LAHH

在达到高高液位时触发的报警。

3.9

高液位 high tank level:H

在最高工作液位与高高液位之间设置的,向操作人员提供警示或报警的关注液位。

3.10

高液位报警 high tank level alarm:LAH

当罐液位达到高液位时触发的报警。

3.11

响应时间 response time:RT

从报警触发开始到执行设定动作(可以是人为操作也可以是自动系统)完成所需的时间。

3.12

最终元件 final element

阀门、泵或其他可以终止流入、防止储罐溢出的设备。

3.13

储罐防溢系统 overfill prevention system:OPS

防止储罐介质溢出的保护系统。

注:OPS可以是技术措施也可以是管理措施,也可以两者皆有。

3.14

手动储罐防溢系统 manual overfill prevention system:MOPS

需要操作人员操作的储罐防溢系统。

3.15

自动储罐防溢系统 automatic overfill prevention system:AOPS

无需操作人员操作的储罐防溢系统。

3.16

危险失效 dangerous failure

对执行安全功能有影响的组件和/或子系统和/或系统的失效,其:

a) 在要求时阻止安全功能的执行(要求模式),或导致安全功能失效(连续模式)以致EUC进入危险或潜在危险的状态。

b) 降低在要求时安全功能正确执行的概率。

[来源:GB/T 20438.4—2017,3.6.7]

3.17

安全失效 safe failure

对于执行安全功能有影响的组件和/或子系统和/或系统的失效,其:

a) 导致安全功能的误动作从而使 EUC(或其一部分)进入或保持安全状态;或

b) 增加安全功能的误动作从而使 EUC(或其一部分)进入或保持安全状态的概率。

[来源:GB/T 20438.4—2017,3.6.8]

3.18

功能安全 functional safety

与过程和 BPCS 有关的整体安全的组成部分,它取决于 SIS 和其他保护层的正确功能执行。

[来源:GB/T 21109.1—2007,3.2.25]

3.19

功能安全评估 functional safety assessment

基于证据的调查,以判定由一个或多个保护层所实现的功能安全。

[来源:GB/T 21109.1—2007,3.2.26]

3.20

随机硬件失效 random hardware failure

在硬件中,由一种或几种可能的退化机理而产生的,在随机时间出现的失效。

注 1:在各种元件中,存在以下不同速率发生的许多退化机理,在这些元件工作不同的时间之后,这些机理可制造公差引起元件发生故障,从而使包含许多元件的设备将以可预见的速率,但在不可预见的时间(即随机时间)发生失效。

注 2:随机硬件失效和系统性失效的主要区别是由随机硬件失效导致的系统失效率(或其他合适的度量)可以用合理的精度来量化,但系统性失效无法精确预计,因此,系统性失效引起的系统失效率则不能精确地用统计法量化。也就是说,由随机硬件失效引起的系统失效率以用合理的精度来量化,但是由系统性失效引起的系统失效率不能精确地用统计法量化,因为导致系统性失效的这些事件无法简单预测。

[来源:GB/T 20438.4—2017,3.6.5]

3.21

安全仪表系统 safety instrumented system;SIS

用来实现一个或几个安全仪表功能的仪表系统。SIS 可以由传感器、逻辑控制器和执行器的任何组合组成。

[来源:GB/T 21109.1—2007,3.2.72]

3.22

安全完整性 safety integrity

在安全仪表系统在规定时段内、在所有规定条件下满足执行要求的安全仪表功能的平均概率。

[来源:GB/T 21109.1—2007,3.2.73]

3.23

安全仪表功能 safety instrumented function;SIF

具有某个特定 SIL 的,用以达到功能安全的安全功能,它既可以是一个安全仪表保护功能,也可以是一个安全仪表控制功能。

注:该术语与 GB/T 21109.1—2007 不同,以体现行业应用习惯。

3.24

安全完整性等级 safety integrity level;SIL

用来规定分配给安全仪表系统的安全仪表功能的安全完整性要求的离散等级(4 个等级中的一个)。SIL4 是安全完整性的最高等级,SIL1 为最低等级。

[来源:GB/T 21109.1—2007,3.2.74]

3.25

安全要求规格书 safety requirements specification;SRS

包含安全仪表系统应执行的安全仪表功能的所有要求的规格书。

注:该术语与 GB/T 21109.1—2007 不同,以体现行业应用习惯。

3.26

检验测试 proof test

为揭露安全仪表系统中未检测到的故障而执行的测试，以便在必要时把系统修复到所设计的功能。

[来源：GB/T 21109.1—2007，3.2.58]

3.27

安全状态 safe state

达到安全时的过程状态。

注1：本文件中的安全状态主要指将不会造成储罐溢流的进料过程状态。

注2：该术语的定义同GB/T 21109.1—2007中的定义有差别，以体现行业应用习惯。

4 缩略语

下列缩略语适用于本文件。

AOPS：自动储罐防溢系统(Automated Overfill Prevention System)

ATG：自动液位计(Automatic Tank Gauge)

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

EMC：电磁兼容(Electro Magnetic Compatibility)

EUC：受控设备(Equipment Under Control)

FMEA：失效模式及后果分析(Failure Mode and Effects Analysis)

FPL：固定程序语言(Fixed Program Language)

FVL：全可变语言(Full Variability Language)

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

HFT：硬件故障裕度(Hardware Fault Tolerance)

LVL：有限可变语言(Limited Variability Language)

MOC：变更管理(Management of Change)

MOPS：手动储罐防溢系统(Manual Overfill Prevention System)

MTTR：平均恢复时间(Mean Time to Restoration)

OPS：储罐防溢系统(Overfill Prevention System)

PE：可编程电子(Programmable electronic)

PFD：要求时危险失效概率(Probability of Dangerous Failure on Demand)

PFH：每小时危险失效平均概率(Average Frequency of a Dangerous Failure Per Hour)

SIF：安全仪表功能(Safety Instrumented Function)

SIL：安全完整性等级(Safety Integrity Level)

SIS：安全仪表系统(Safety Instumented System)

SRS：安全要求规格书(Safety Requirements Specification)

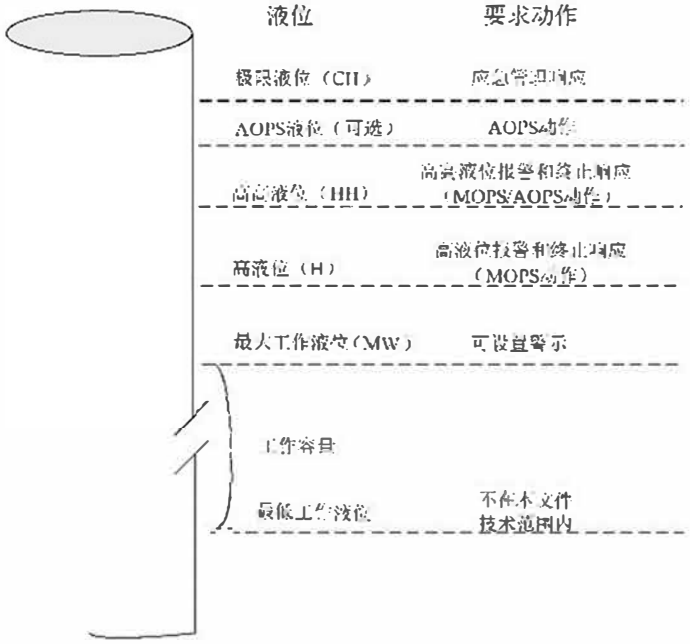
UPS：不间断电源(Uninterruptible Power Supply)

5 储罐防溢系统通用要求

5.1 一般要求

5.1.1 储罐防溢系统应包括技术措施和管理措施。

5.1.2 储罐防溢系统技术措施可包括高液位报警、液位超高联锁等。典型的技术措施设置见图1。



注：图1技术模型来源于行业良好工程实践经验。

图1　储罐防溢系统通用技术模型

5.1.3　储罐防溢系统管理措施可包括储罐技术档案、储罐容积表、运行日报表、操作规程等。相关要求如下：

——应设置“一罐一档”，储罐技术档案应至少包括罐的类型、储存介质、储罐材质、储罐关注液位、标称容积、位号、测量仪表、附属部件、投运时间、维检修时间、已设置的保护措施等；

——储罐运行日报表应实时更新罐内已存量并计算可用容积。进料过程中应实时监视进料流量变化情况和罐内液位变化情况。

5.1.4　应通过风险分析确定为满足可容忍风险储罐防溢系统需要实现的降险能力，通过安全要求分配确认液位报警、液位超高联锁的设置以及安全完整性等级的要求。

注：不同环境、不同介质、不同容量的储罐，储罐溢流的后果和风险不同。

5.1.5　应通过手动操作的有效响应或设备自动联锁实现进料停止。

注：在本文件中“停止”包括如下含义：

1）　关掉压力源（例如，停泵）；

2）　转移进料；

3）　切断流量（关闭进料阀门）；

4）　使用其他方法将进料过程导入安全状态。

5.1.6　应建立罐区安全管理体系（见第6章）和储罐溢流事故应急预案（见第6章）。

5.1.7　液位监测和高液位报警可通过连续液位计或自动储罐计量系统实现。

5.1.8　独立的高高液位报警应由液位传感器和报警系统构成。

5.1.9　AOPS联锁功能应由液位传感器、控制器、执行单元实现。

5.2　储罐监控方式及防溢系统仪器仪表配置分类

根据储罐具体使用情况可将储罐监控方式和防溢系统仪器仪表配置分为四类，见表1。

表 1 储罐监控方式和防溢系统仪器仪表配置分类表

分类	1 类	2 类	3 类	4 类
监控	1. 现场监控； 2. 人员在收油的第一个小时内持续在场； 3. 在收油期间每个过程的定期在场； 4. 收油的最后 1 h 内持续在场	1. 人员在收油的第一个小时内持续在场； 2. 在收油期间每小时在场； 3. 收油的最后 1 h 内持续在场	1. 在收油的第一个 30 min 内持续在场； 2. 在收油的最后 30 min 内持续在场	无现场监控要求。 对无人值守的罐区，在收油期间由操作员、运输者或控制室进行持续监控
仪器仪表配置情况	现场仪表	一个液位仪表(远程)	一个液位仪表(远程)	两个液位仪表[ATG 监控和独立高高(HH)液位报警]
进料阀门设置	手动阀门	手动阀门	远控阀门	远控阀门
报警及联锁设置	无报警无联锁	可设置报警，人员需现场进行响应	报警发送至控制室，未设置独立的 AOPS	液位报警和液位联锁独立发送至控制室，设置独立的 AOPS

5.3 储罐防溢系统全生命周期功能安全要求

应对储罐防溢系统实现全生命周期功能安全管理。全生命周期功能安全要求应包括：

——储罐防溢安全管理要求(见第 6 章)；
——储罐溢流风险评估要求(见第 7 章)；
——储罐防溢系统安全要求分配的要求(见第 8 章)；
——储罐防溢系统设计要求(见第 9 章)；
——储罐防溢系统安装要求(见第 10 章)；
——储罐防溢系统运行前安全确认要求(见第 11 章)；
——储罐防溢系统的验收要求(见第 12 章)；
——储罐防溢系统检验测试和维护要求(见第 13 章)；
——储罐防溢系统变更管理要求(见第 14 章)；
——储罐防溢系统停用要求(见第 15 章)。

6 储罐防溢安全管理要求

6.1 一般要求

储罐管理制度中应包括储罐防溢安全管理要求，内容包括：

——操作规程，包括针对正常和异常操作条件的措施和规程；
——应急响应程序及现场处置预案；
——操作和维护人员的能力培养和维持；
——由合格的人员对功能性设备系统进行测试和维护；
——储罐防溢系统仪表和设备的定期检查和维护计划；
——人员和硬件变更的管理(MOC)；
——有关未遂事故和事故的判断、调查、沟通；
——处理未遂事故或减轻事故影响的后续跟进；
——良好操作实践和事故教训分享；

——异常和正常条件下，业主/运行方组织内以及承运方和业主/运行方之间的沟通保障体系。

注：承运方是指按照合同要求将介质运输至指定地点的相关方。业主是指储罐的资产所有者。运行方是指按照合同要求运行和管理储罐的相关方。有时承运方和业主、运行方可能是一方。

6.2 关注液位管理和定期复审要求

6.2.1 业主/运行方应按照9.2要求建立关注液位并进行管理。

6.2.2 关注液位应按照储罐防溢系统要求定期审查（按照SIS检验测试周期及大罐维修周期），以确保其设定值在当前工况下适用。

6.2.3 储罐发生物理变更、操作变化或储罐防溢系统发生变化时，应开展关注液位复审。

注1：常见的物理变更包括：内/外浮顶更换，罐壁外扩，罐底板更换，增加辅助设备，计量设备变化，侧通风口的变化，罐密封件尺寸的变化等。

注2：常见的操作变化包括：介质变更，输入/输出管线变更，最大流量变更，储罐完整性发生变化后仍继续运行（如罐壁腐蚀后，降低液位继续运行），操作方式变更（如并联、旁接、连续掺混等），员工、权限、操作或设备变更引起的响应时间变更等。

注3：储罐防溢系统变化包括：报警响应发生变化，AOPS联锁功能变更等。

6.3 储罐防溢系统的功能安全评估要求

储罐防溢系统的功能安全评估活动可参考GB/T 32202执行。

6.4 储罐防溢安全管理体系要求

6.4.1 储罐防溢安全管理体系文件要求应至少包括工艺安全信息、工艺危害分析、功能安全评估、变更管理、操作规程、机械完整性、设备变更、作业许可证、事故调研、员工参与。

6.4.2 应对储罐防溢安全管理体系文件进行定期复审。

6.5 储罐防溢操作安全规程要求

6.5.1 制定进料计划的规程

6.5.1.1 应制定进料计划，内容应包括储罐进料的正常操作和填充储罐到最高工作液位的规程，还应包括一些复杂操作，如：

——在同一进料作业中切换接收罐；

——多个储罐同时进料；

——多个来源同时向某一储罐进料；

——其他非正常工况。

6.5.1.2 计划中应明确进料量，与接收罐的可用容积比较，确保储罐有足够的可用容积。

注：接收罐的可用容积使用MW来计算。

6.5.1.3 应在进料前做好充分计划，在液位达到MW前及时切罐或停止进料。

6.5.1.4 计划中应明确进料完成时储罐预期液位，未经授权预期液位不应超过MW。在任何情况下，储罐进料后的液位均不应达到或超过HH或AOPS液位。

注：AOPS液位指需要由AOPS执行动作的液位值。

6.5.1.5 计划中应明确进料过程中各岗位人员职责分配。

6.5.2 进料前的活动规程

6.5.2.1 进料前应核查储罐中的可用容积，与计划的进料量/卸料量（如油罐车卸油操作）进行比较，如果计划的进料量超过储罐的可用容积，应调整计划。

6.5.2.2 进料前，应至少明确以下信息并形成文档记录：

——计划进料量；

——计划进料开始时间和预计结束时间；

——预计流量，包括任何可能的工况变化。

6.5.2.3 进料前，应核对罐区所有阀门状态，以确保介质被输送到指定储罐中。连接不同储罐的同一进料管道只应打开待进料储罐的入口阀门，其他所有储罐入口阀门应关闭。

6.5.2.4 对于1类、2类、3类储罐，在进料前应确认收料操作人员与上游操作人员间通信畅通，确保进料过程中必要时有足够的响应时间停止进料。

——对于1类储罐，参与人员可在进料开始时至少通信一次，在进料过程中定期通信，并在进料结束之前至少通信一次。

——对于2类和3类储罐，参与人员应至少在进料过程的开始和结束时进行通信。

6.5.2.5 在进料前应确认监控系统处于正常工作状态。

6.5.2.6 在进料期间，储罐所在区域防火堤的排水阀应保持关闭。

6.5.3 进料期间的活动规程

6.5.3.1 应在进料期间对储罐液位定期进行监测，并记录。

6.5.3.2 在进料期间，应定期对以下信息的实际值与计划中的期望值进行比较：

——参与进料的储罐；

——进料或卸料速率；

——未完成的进料量；

——剩余的罐可用容积；

——预计进料完成的时间。

6.5.3.3 应监测连接同一进料管道的其他储罐，确保没有非正常的液位变动。

6.5.3.4 在进料过程中，应确保换班的操作人员之间保持通信和控制的连续性。

6.5.3.5 进料开始后，应立即验证介质是否只流入正确的储罐中，且储罐防溢系统相关措施有效。

6.5.3.6 在进料期间，应定期巡检，确保管道、储罐、泵、防火堤等设施的完整性，并确保现场未发生可能影响进料的未经授权的活动。

注：此要求不适用于无人值守的4类储罐。

6.5.4 进料后的活动规程

在进料结束后，应确保阀门及动力设备(如泵)顺序关闭。

6.5.5 进料过程的文档化

6.5.5.1 在进料结束时，应记录以下内容并注明时间和日期：

——进料涉及的储罐；

——实际进料量；

——进料后的储罐液位。

6.5.5.2 所有与进料相关的记录应保存一段时间，时间长短应符合相关法律法规及业主/运营商相关管理制度。

6.5.6 异常情况的活动规程

6.5.6.1 储罐正常进料不宜超过最高工作液位(MW)。

6.5.6.2 储罐针对以下异常情况应建立活动规程：

——报警触发(例如，高液位报警后，现场人员如何响应实现进料停止)；

——溢流后的响应；

——液位监控或报警通信中断，或与储罐防溢系统相关的公用设施故障；

——操作、设备、环境、天气等出现异常情况；

——计划进料流量和检测到的实际进料流量之间偏差超出5%时。

6.5.6.3 针对储罐液位监测系统或储罐防溢系统故障情况，应设置恢复时间要求，启动预先建立的异常操作程序。程序应规定在储罐进料作业前现场须设置有足够的风险降低补偿措施。在液位监测系统故障解除前，进料作业的所有操作都应经过审核。

6.6 储罐溢流事故应急预案要求

6.6.1 储罐区应设置应急预案，并定期进行演练。

6.6.2 应急预案的设置应符合国家、行业或企业相关标准规范要求。

6.6.3 现场处置方案应符合现场实际并具有可操作性。方案编制应符合 GB/T 29639。

7 储罐溢流风险评估

7.1 一般要求

7.1.1 应在新建储罐进行防溢系统设计前或在役储罐变更设计前开展一次储罐溢流风险评估。

注：风险评估包括定量或半定量方法，目前常用的方法为 HAZOP、FMEA 等。

7.1.2 开展风险评估的组织及人员资质、组织管理、实施流程、文档化和发布签署等应符合国家相关文件要求和国家、行业、企业相关标准及规范要求。

7.2 风险评估实施要求

7.2.1 应制定明确的风险可接受准则，该准则应符合国家、行业或企业相关标准规范要求。

7.2.2 应针对罐区工艺、设备、设施、人员等方面评估会导致储罐溢流事件发生的所有合理可预见情况，包括仪表或阀门故障状况、误用、人员误操作、异常的进料运行模式等。

7.2.3 应针对所有已辨识出的潜在危险事件，确定合理可预见的储罐溢流后果。

7.2.4 应评估会导致储罐溢流的危险事件的发生频率（或频率等级），频率或频率等级的定义和选择应符合国家、行业或企业相关标准规范要求，并具有可信的来源。

7.2.5 应评估危险事件会导致的储罐溢流后果严重性程度，后果及其严重性等级的定义和选择应符合国家、行业或企业相关标准规范要求，并具有可信的来源。

7.2.6 应评估储罐溢流的风险等级，风险分级准则应符合国家、行业或企业相关标准规范要求。

7.2.7 对提出的风险降低措施（如液位报警、联锁），应有明确的实施和追踪的负责人。

7.2.8 应详细记录 7.2.1～7.2.7 各项活动所分析及引用的资料的名称及版本号。

7.2.9 应详细记录 7.2.1～7.2.7 各项活动内容，形成文档，并由相关责任人签署。

7.2.10 风险评估文档应包括：

——风险评估方法；

——风险的确定、风险的减轻和风险的可接受性；

——团队成员及其专业知识；

——概率、后果因素及风险评级；

——评估的基础，包括假设、数据来源和数据分析；

——如何将风险降低到可接受的水平，以满足业主/运营方的标准。

7.2.11 当罐体、罐区及周围区域发生变化增加溢流风险时，应重新开展风险评估。

7.2.12 业主/运行方应按照国家相关文件要求和标准规范定期开展风险评估。重点监管危险化学品和危险化学品重大危险源的生产储存装置不得超过 3 年，其他生产装置不宜超过 5 年。

8 储罐防溢系统安全要求分配

8.1 一般要求

8.1.1 安全要求分配应在开展过一次风险评估后展开。

注：目前常用的安全要求分配方法包括保护层分析(LOPA)、风险矩阵、风险图等。

8.1.2 安全要求分配应包括储罐防溢安全功能要求确定和安全完整性要求分配。

8.1.3 开展安全要求分配的组织及人员资质、组织管理、实施流程、文档化和发布签署等应符合国家相关文件要求和国家、行业或企业相关标准规范要求。

8.2 安全要求分配实施要求

8.2.1 应明确定义用于预防、控制或减轻储罐溢流风险的保护层及其安全功能，包括由安全仪表系统执行的安全仪表功能(SIF)。

8.2.2 应评估并识别 AOPS 联锁功能与液位监测及报警功能之间存在的潜在的共因失效。

8.2.3 应评估并识别储罐防溢系统与储罐溢流触发事件或原因之间的相关性和独立性。

8.2.4 应评估储罐防溢系统中各保护功能的风险降低能力。各保护功能风险降低能力的定义和选择应符合国家、行业或企业相关标准规范要求，并具有可信的来源。

8.2.5 如果评估确定需要设置 SIF(如独立的 AOPS 联锁功能)，应分析 SIF 的安全功能要求和安全完整性等级要求。

8.2.6 应确定 SIF 最大可接受误动作率要求(如需要)。

8.2.7 应确定单个或多个 SIF 动作可能带来的附加危害。

8.2.8 对动力源(如电源、液动源或气动源)中断而不进入安全状态的 SIF，应根据 9.4.3.11 采取行动。

8.2.9 SIL 要求应结合罐区实际情况合理分配。在设置了合理的报警功能、BPCS、AOPS 后，若储罐溢流风险仍未降至可接受范围，宜设置独立于 SIS、BPCS 的声光报警系统。

8.2.10 应详细记录 8.2.1～8.2.9 各项活动中所分析及引用的资料的名称及版本号。

8.2.11 应详细记录 8.2.1～8.2.9 各项活动内容，形成文档，并由相关责任人签署。

8.2.12 安全要求分配文档应包括：

——安全要求分配方法；

——风险可容忍标准的确定；

——团队成员及其专业知识；

——初始事件频率、场景后果及残余风险确定；

——评估的基础，包括假设、数据来源和数据分析；

——为满足风险可容忍标准需采取的行动(即安全要求分配结果)。

9 储罐防溢系统设计要求

9.1 一般要求

9.1.1 储罐系统设计应符合国家相关法律法规及设计规范要求，储罐防溢系统应根据储罐溢流的风险评估(第 7 章)及安全要求分配(第 8 章)的结果进行设计。

9.1.2 业主和运行方应按照每个储罐的具体参数、使用条件等方面合理设计储罐防溢系统。设计要考虑的因素包括：储罐的类型(操作模式、管理方式)、各液位参数、报警和控制系统、报警信号、UPS、联锁功能及安全防护等因素。

9.2 关注液位的设计

9.2.1 建立关注液位

9.2.1.1 在进行储罐防溢系统设计前，应定义储罐的关注液位，至少包含以下三个液位参数，见图 2。

——极限液位(CH)；

——高液位(H)；

——最高工作液位(MW)。

注：此处 7.7 cm 是根据行业良好工程实践得出。

图 2　储罐关注液位

9.2.1.2　3 类及以上储罐的关注液位除应满足 9.2.1.1 要求外，还应包括高高液位（HH）。储罐监控方式分类与关注液位设置对应关系，见表 2。

表 2　储罐监控方式分类与关注液位设置对应表

分类	1 类	2 类	3 类	4 类
关注液位	MW、H、CH	MW、H、CH	MW、H、HH、CH	MW、H、HH(AOPS)、CH

9.2.1.3　在确定关注液位参数时，应关注以下内容：

——存储的介质特性；

——日常的操作参数（包括阀门及管道等的操作参数）；

——介质的发送、接收、传输的量及流速。

注：现场对警示及报警的响应能力。本文件中响应能力需考虑响应动作及响应时间。

9.2.1.4　极限液位计算时，应关注下述参数：

——有效罐壁高度；

——罐壁最高点至泡沫喷嘴底部；

——有效浮顶高度；

——罐壁最高点到纵梁的深度；

——自液面到附件的高度；

——自液面到浮顶支撑高度；

——浮顶支撑固定销之间的距离；

——附件到罐壁的距离；

——罐壁到浮顶支撑的距离；

——浮顶的坡度。

注：极限液位通常由储罐设计单位计算并反映在设计文件中，称为储罐设计液位。

9.2.1.5　储罐发生下述事项时，应审核是否对极限液位产生影响，并完成变更管理：

——储罐完整性发生变化（包括罐本体及附件）；

——维修罐壁；

——密封超过通风口或储罐上边沿；

——其他可能影响极限液位的更改。

9.2.1.6 AOPS 液位应设置在高高液位(HH)或以上，且应低于极限液位(CH)，AOPS 液位与 CH 间的差值应基于当前罐在最大流速下触发 AOPS 系统和停止进料所需的响应时间来计算。AOPS 液位与 CH 间的液位差不应小于 7.7 cm。

注：当储罐同时作为泄放装置使用时，与其连接的泄放管线阀门都需要处于铅封开启(CSO)或锁定常开(LO)位置，此情况下采用 AOPS 措施需要在考虑储罐防溢的同时考虑泄放措施的有效性。

9.2.1.7 高液位(H)应设置于最高工作液位(MW)与极限液位(CH)之间，当关注液位设置有高高液位(HH)时，H 应设置于 HH 以下。

9.2.1.8 MOPS 液位宜设置在 H 处。H 与 HH 之间差值应基于当前罐在最大流速下人工停止进料所需的响应时间。

注：MOPS 液位指需要由 MOPS 执行动作的液位值。

9.2.1.9 高高液位(HH)应设置在极限液位(CH)以下，其间的差值应由最大进料流速时操作人员或 AOPS 终止进料所需的响应时间确定，但距离不得小于 7.7cm。

9.2.1.10 响应时间计算应包括 9.2.1.18 中提及的因素。应计算出响应时间过程对应的进料体积(响应时间×最大流速)后，使用罐容表或等效的计算方法来确定罐中与该进料体积对应的垂直距离。

注：如罐有多个管线同时进料，则在计算进料体积时，要将多个管线的进料体积求和。

9.2.1.11 储罐液位达到 HH 时应采取措施使其尽快降低到 MW。

9.2.1.12 在确定 HH 时除响应时间外还应关注进料体积裕度，主要包括：

——可能出现的泄放量(如储罐同时用作泄压时，在停止进料后可能发生泄压时所产生的进料体积)；

——在通信故障或阀门失灵的情况下，由高位管线倒排回油罐的体积；

——当液位达到高高液位(HH)时，为将液位降至最高工作液位(MW)以下，转移罐内介质的速率。

9.2.1.13 并联运行的储罐在设置高高液位(HH)时，应确保储罐标高或运行高度不同的情况均适用。

示例：储罐并联运行时高度或标高不同，那么某一储罐可能比其他先"满"(达到其溢流液位)。

9.2.1.14 最高工作液位(MW)宜设置警示。

9.2.1.15 最高工作液位(MW)与高液位(H)报警之间的距离应设置足够，确保进料时不会在如下情况触发不必要的高液位报警：

——产品因热膨胀提升液位；

——物料晃动造成的液位高度增加。

9.2.1.16 对于作为管道泄压罐的储罐，应在 HH 和 CH 以及 MW 和 HH 之间均留出泄放余量。

9.2.1.17 储罐的各项关注液位参数应告知操作人员及巡检人员，并明示于罐底人工巡检位置、罐顶人工测量口及控制室。

9.2.1.18 响应时间应根据不同的关注液位进行计算，其定值取决于各关注液位的高度设定及要求的响应动作，应关注以下内容：

——手动响应时间计算应包括：

- 启动报警需要的时间；
- 操作人员确认报警(避免误报的情形)的时间；
- 完成设计的响应操作所需的时间(如关阀操作)；
- 执行响应动作的时间(如阀门关闭过程时间)；
- 操作人员确认及可能采取补救所需的时间，相关活动包括：确认所有系统部件都已正确响应，若系统未正确响应应采取适当补救动作；
- 转移罐内介质的速率；

——自动响应时间计算应包括如下因素：

- 启动储罐防溢系统需要的时间(包括信号的传输、执行设备按照设计进行动作并完成响应动作的时间)；

- 验证所有系统部件都已正确响应的时间，以及若系统未正确响应时采取适当补救动作的时间；
- 转移罐内介质的速率。

9.2.2 建立关注液位文档

应建立文档记录 9.2.1 要求的各关注液位确定的依据及相关过程数据。关注液位发生变化或确定液位过程中的相关参数发生变化时，应及时更新文档。

9.3 储罐防溢系统的分类及组成

9.3.1 储罐防溢系统分类

根据系统触发后的响应方式将储罐防溢系统分为两类：手动防溢系统（MOPS）和自动防溢系统（AOPS）。

9.3.2 手动防溢系统（MOPS）

9.3.2.1 MOPS 应通过操作人员的响应终止进料。

注：以下情况都属于 MOPS 的响应动作：操作人员去现场进行开关阀门或其他设备的操作，或在控制室触碰按钮来实现阀门或其他设备的远程开关。

9.3.2.2 MOPS 设备组成包括但不限于：

——传感器（例如，液位计、液位开关）；
——数据传输设备；
——报警信号系统；
——逻辑控制器（例如，继电器、PLC、SIS）；
——手动阀门。

9.3.3 自动储罐防溢系统（AOPS）

9.3.3.1 AOPS 响应过程无需人员干预或参与，应通过储罐液位传感器、逻辑控制器和最终执行元件组成的自动控制回路实现自动终止进料。

9.3.3.2 AOPS 设备组成包括但不限于：

——传感器（例如，液位计、液位开关）；
——逻辑控制器（例如，继电器、PLC、SIS）；
——远控阀门（例如，气动、电动、液动）。

9.4 AOPS 的功能安全设计

9.4.1 一般要求

应基于安全要求分配（第 8 章）确定 AOPS 是否应由 SIS 实现。对于由 SIS 实现的 AOPS 应确定其安全完整性要求，编制安全要求规格书（SRS），依据 SRS 完成 AOPS 设计。

注：9.4 中 AOPS 特指需要由 SIS 实现的储罐防溢安全仪表功能。

9.4.2 SRS 要求

9.4.2.1 SRS 应包括以下内容：

——由 SIS 实现的 AOPS 的描述；
——与 AOPS 相关的现场输入和输出设备清单（如位号、厂家、型号等）；
——识别和考虑 AOPS 与液位监测、报警等措施共因失效的要求；
——AOPS 的过程安全状态定义，例如，关阀以停止进料，不会造成储罐溢流的状态；

注 1：对于兼具泄压功能的 AOPS，其安全状态定义要结合泄放需求综合评判。

——任何单个的过程安全状态定义，当这些状态同时发生时就会产生一个单独的危险（如事故应急池的多来源同时泄放，可能产生应急池的溢流危险）；
——AOPS 的要求源（触发事件）及要求频率的假定来源（如储罐液位超高的初始事件及发生频率假定）；
——检验测试间隔要求；
——检验测试规程相关要求；
——AOPS 的响应时间要求；
——AOPS 要求的安全完整性等级和操作模式（AOPS 一般为低要求模式）；

注 2：操作模式包括低要求模式、高要求模式和连续模式。其中低要求模式指 SIF 只有在要求时才动作，以将储罐运行导入不会溢流的安全状态，并且要求的频率不大于一年一次；高要求模式指将储罐运行导入不会溢流的安全状态的 SIF 仅当要求时才执行，并且要求的频率大于每年一次；连续模式指 SIF 将储罐运行保持在安全状态是正常运行的一部分。

——AOPS 液位测量、范围、精度和触发值的描述；
——AOPS 输出动作和成功操作准则的描述，例如，进料切断阀的要求；
——输入和输出之间的功能关系，包括逻辑功能、数学功能和任何要求的许可；
——AOPS 失效后的人工触发要求；
——得电或失电动作有关的要求；
——AOPS 触发后的复位要求；
——AOPS 最大允许误动作率；
——AOPS 失效模式和要求的 SIS 响应（如报警、自动触发联锁）；
——与 AOPS 启动规程和重新启动规程有关的任何特殊要求；
——AOPS 和任何其他系统（包括 BPCS 和操作员）之间的所有接口；
——旁路要求，包括旁路管理控制要求和旁路清除要求；
——在检测到 AOPS 发生故障时，达到和保持不发生溢流的安全状态所必需的动作规范，并应关注相关人员因素；
——在考虑到运输时间、位置、备件安装、服务合同、环境约束时，AOPS 切实可行的平均恢复时间 MTTR；
——需要避免的 AOPS 输出状态的危险组合的识别；

示例：安全状态为先停泵后关阀，若先关阀后停泵可能导致危险。

——应识别 AOPS 可能遇到的所有极端环境条件；

注 3：需考虑的因素：温度、湿度、污染、接地、电磁干扰/射频干扰、冲击/振动、静电放电、用电区等级、水淹、雷电等。

——AOPS 及其组成设备可能存在的运行模式（如正常运行、维检修、传感器校准等）及各运行模式下可能需要新增的其他风险降低补偿措施；
——任何能经受一次重大意外事故的 AOPS 要求的定义，例如，在一次火灾事故中阀门保持可操作性的时间要求。

9.4.2.2 应关注自动联锁切断功能的可操作性和可维护性。

9.4.2.3 对于在线测试和可能产生报警的功能，应设置旁路设施。

9.4.3 设计和实施要求

9.4.3.1 AOPS 设计和实施应以安全要求规格书为依据，并满足本条所有要求。

9.4.3.2 对于同时实现安全仪表功能和非安全仪表功能的 SIS，所有在正常和故障状况下会对 AOPS 有负面影响的部分（包括但不限于硬件、嵌入式软件和应用程序）都应当成 SIS 的组成部分，并应符合最高 SIL 要求。

注 1：除非特殊情况，尽量保持液位监测、高液位报警和 AOPS 之间充分的独立性。

注 2：充分的独立性意味着任何非安全仪表功能或编程实现的非安全嵌入式软件或应用程序功能都不会引起安全仪表功能失效。

9.4.3.3 SIS 承担的其他 SIF 与某一 AOPS 预防同一危险事件时，共享或共用硬件、嵌入式软件或应用程序实现的 SIL 能力应高于该 AOPS 的 SIL。

示例：以某储罐高高液位 AOPS 为例，其 SIL 要求为 SIL2，在高液位还设置了具有 SIL1 要求的其他 AOPS，两者共用 SIS 控制器和最终执行元件，高液位 AOPS 执行单元失效将导致高高液位 AOPS 同时失效，则共用的 SIS 控制器和最终执行元件及相关软件或应用程序应实现高于 SIL2 的能力。

9.4.3.4 SIS 承担的其他 SIF 与 AOPS 预防不同危险事件时，共享或共用硬件、嵌入式软件或应用程序实现的 SIL 能力应不低于该 AOPS 的 SIL。

示例：某储罐 AOPS 所在 SIS 同时承担储罐液位超低联锁功能，AOPS 与液位超低联锁功能共用最终执行元件，经保护层分配确定 AOPS 应实现 SIL2 的能力，液位超低联锁应实现 SIL1 的能力，则共用部分应至少实现 SIL2 的能力。

9.4.3.5 应在设计中解决可操作性、可维护性、诊断、检查和可测试性要求从而降低危险失效可能性。

9.4.3.6 SIS 设计时应关注人员能力和局限性以及分配给操作员和维护人员任务的适宜性。操作界面的设计应良好满足人员习惯并与操作员能接受的培训水平相适宜。

9.4.3.7 AOPS 应设计成只要它把过程置于某个安全状态，它就会保持在安全状态直到启动一次复位为止，安全要求规格书另有规定的情况除外。

9.4.3.8 应设置独立于 SIS 控制器的手动机制来触发进料停止功能，进料切断阀应能实现紧急切断。

9.4.3.9 AOPS 设计应关注与 BPCS 以及其他保护层间的独立性和相关性。

9.4.3.10 基本过程控制系统的控制单元如果不符合 GB/T 21109.1—2007 的要求，则应独立于 SIS 设计，不应影响 AOPS 的功能完整性。当能表明基本过程控制系统的一次失效不会对 AOPS 产生负面影响时，AOPS 的传感或执行设备也可用于基本过程控制系统的功能。

注 1：储罐防溢系统中基本过程控制系统一般承担液位监控、进料操作、工艺调节、液位报警等功能。

注 2：基本过程控制系统与 SIS 交换操作信息但不能影响 AOPS 的功能安全。

注 3：当 AOPS 的一部分同时用于液位监控和调节时，增加的溢罐风险与共用设备（如液位计或进料切断阀）的危险失效率有关，即共用设备发生故障时，将增加溢罐风险，从而对 AOPS 产生一次要求，而 AOPS 由于此共用设备的故障已无法作出响应，因此在上述情况下，需进行额外的分析以确保共用设备的危险失效率足够低。

9.4.3.11 若 AOPS 设备（如进料切断阀、泵）动力源（如电源、液动源或气动源）中断不会进入安全状态，应对动力源丢失和 SIS 动力回路完整性进行监测和报警（如动力线路、电压、液压或气压监视）并根据 9.4.3.14 采取行动。

注 1：常通过使用辅助动力源（如备用电池、不间断电源、储气罐、液压蓄能器、第二气源）来提高动力源完整性。

注 2：动力源中断可能影响多个 SIF，甚至多个 SIS。因此要考虑多个 SIF 的共同原因失效。

9.4.3.12 AOPS 的设计应针对识别出的信息安全防护风险提供必要的弹性。

注：AOPS 信息安全防护相关导则见 IEC 62443-2-1:2010。

9.4.3.13 安全手册应包括 AOPS 相关的操作、维护、故障检测和约束条件等内容，应阐明 AOPS 预期的设备配置和预期的运行环境。

注：安全手册可能是一份独立文档，也可能是一份文档集。安全手册定义了如何安全应用 SIS 相关设备的信息。声明符合 GB/T 20438 的 SIS 相关设备，安全手册由制造商提供。

9.4.3.14 当检测（通过诊断测试、检验测试或其他方式）到 AOPS 存在一个危险故障时，应采取补偿措施来维持安全运行。如果不能维持安全运行，则应采取特定的动作来达到或保持储罐的安全状态。当补偿措施依赖于操作员根据报警来采取特定动作时（如打开或关闭阀门），应将报警作为安全仪表系统的一部分。

注：维持安全运行所需的补偿措施取决于安全完整性要求、溢流事件的可容忍风险、AOPS 硬件故障裕度、预期的故障维修时间以及其他储罐防溢保护层的可用性。

9.4.3.15 若 AOPS 的危险故障都是通过报警来提醒操作员，故障报警应符合 AOPS 的检验测试和变更管理要求。

9.4.4 硬件故障裕度（HFT）

9.4.4.1 HFT 可被分配给组成 AOPS 的子系统（如传感、控制、执行）。

9.4.4.2 AOPS或者AOPS的子系统HFT应符合：

——GB/T 21109.1—2007中11.4；

——GB/T 20438.2—2017中7.4.4.2(路线1H)；

——GB/T 20438.2—2017中7.4.4.3(路线2H)。

9.4.5 AOPS设备的选型要求

9.4.5.1 下列行为应符合GB/T 20438.2—2017和GB/T 20438.3—2017以及9.4.6的要求：

——选择AOPS的组成设备；

——把设备集成到SIS架构中；

——根据SRS制定设备的验收准则。

9.4.5.2 应根据SRS要求、PFD计算过程中假设的可靠性参数以及运行环境要求选择AOPS组成设备。

注：设备厂商需提供不同运行环境和不同运行模式下的失效率，如频繁使用情况和长期不用情况下的失效率数据不同，洁净环境下和恶劣环境下的失效率数据可能也不同。

9.4.5.3 根据以往使用的情况选择AOPS组成设备应符合下列要求。

——应开展以往使用评估以证明设备适用于当前AOPS。

注1：经以往使用评估得出的数据可以补充到用于计算随机失效的数据库。

——以往使用评估应收集证据证明：与要求的安全完整性相比，系统性危险故障已被降低至充分低的水平。证据的详细程度取决于所评估设备的复杂程度。

——以往使用评估应收集：设备在相似运行环境中的性能信息，以往使用中已安装设备的功能性和完整性，包括过程接口、设备边界、通信和公共设施。

——以往使用评估应对以下内容进行评估：

- 制造商的质量体系、管理体系和配置管理体系；
- 设备充分的标识和规范；
- 在类似运行环境中设备性能的证明；

注2：在现场设备(例如，传感器和最终元件)满足某一给定规范的情况下，该设备在安全应用和非安全应用中的行为通常是一样的。因此，类似设备在非安全应用中的性能证明也能用于满足此需求。

- 大量的运行经验。

注3：一般通过用户设备清单记录现场设备与操作经验有关的信息，该清单的形成是基于设备在安全和非安全应用中成功运行的大量历史记录，不包括未能成功执行功能的设备。倘若下列条件均满足，现场设备清单能用于支持运行经验的声明：

a) 定期更新和监视清单；

b) 只有在获得足够的运行经验时，现场设备才能加入该清单；

c) 当现场设备的运行历史记录显示出它们不能完美地执行功能时，从该清单中删除它们；

d) 清单中要包含相关的运行环境。

注4：设备性能受到运行环境的影响较高，通常推荐基于大量安装并运行足够长时间而获得的充分的设备性能表现来进行选择。获得的运行经验需允许足够时间来揭露早期失效，例如和规格书、储存、安装及试运行相关的早期失效。

注5：用于获得可信的具有统计意义的可靠性数据而需要的运行经验通常远多于用于证明"以往使用"需要的运行经验。

——所有基于"以往使用"选用的设备应通过特定的版本号进行识别，并受控于变更管理程序。当对这些设备做出变更时，应对"以往使用"的证据是否继续有效进行论证(通过评估变更的影响)。

9.4.5.4 对于SIL1、SIL2、SIL3的AOPS，基于"以往使用"选择FPL设备(如智能液位变送器)应满足9.4.5.1～9.4.5.3及以下要求。

——应识别并考虑所有可能影响AOPS安全的设备组态选项。对于没有定义特定设置的，应确认设备的默认设置是否合适。设备未被使用的特性应在适用性证据中加以识别，并确定这些特性不太可能危害到AOPS。

——对于设备的特定组态和运行环境，适用性证据应包括：

- 输入和输出信号的特点；
- 使用的模式；
- 使用的功能和组态；
- 以往在类似操作环境中的使用情况。

——对于 SIL 3 应用，应对 FPL 设备进行评估，评估内容参见 GB/T 21109.1—2007 中 11.5.4.4。

9.4.5.5 对于 SIL1 或 SIL2 要求的 AOPS 中使用的 PE 设备，基于"以往使用"选择 LVL 设备时应满足 GB/T 21109.1—2007 中 11.5.5.6 要求。

9.4.5.6 当 PE 逻辑控制器使用的是 FVL 对应用程序进行编程时，PE 逻辑控制器应符合 GB/T 20438.2—2017 和 GB/T 20438.3—2017 的要求。

9.4.5.7 AOPS 现场设备在选型时应充分考虑工艺操作条件和环境条件，确保因操作环境影响而导致的失效降至最低水平。考虑的条件应包括：腐蚀、物料在管道中冻结、悬浮物、温度和压力极限、环境相对湿度极限、干式取压管中的冷凝、湿式取压管中的不充分冷凝等。

9.4.5.8 "得电触发"的离散输入/输出电路应采取措施确保电路和电源的完整性。

注 1：此方法的例子是使用一个线路终端监视器，在这种情况能连续监视一个辅助电流从而确保电路的连续性，而辅助电流的幅度不会影响 I/O 的正常工作。

注 2："失电触发"的附加要求参见 9.4.3.11。

9.4.5.9 智能传感器应进行写入保护以防止远程意外修改，除非经安全审查允许使用读写功能。

注：复审要考虑人员因素，例如，未遵守规程。

9.4.6 接口设计要求

9.4.6.1 一般要求

AOPS 的接口包括但不限于：

——操作员接口；

——维护/工程接口；

——通信接口。

9.4.6.2 操作员接口要求

9.4.6.2.1 对于 SIS 操作员接口与 BPCS 操作员接口共用的情况，应关注 BPCS 操作员接口中可能发生的可信失效。

注：这包括编制计划，使得在操作显示界面完全失效的情况下，有序地安全停车。

9.4.6.2.2 应对旁路开关或其他旁路手段设置保护，以防止未授权的使用（例如，通过钥匙锁或密码与管理控制相结合）。

注：需考虑对旁路操作实施强制时间限制，并限制每次激活的旁路数量。

9.4.6.2.3 对于维护 AOPS 至关重要的 SIS 状态信息应在操作员界面显示。这些信息包括：

——目前处于 AOPS 动作序列中的哪个环节；

——已发生 AOPS 保护动作的指示；

——某个保护功能被旁路的指示；

——已发生某个自动动作（如表决降级和/或故障处理）的指示；

——传感器和最终元件的状态；

——影响安全的动力源丧失（如 UPS 故障）；

——诊断结果；

——支持 SIS 所需的环境改善设备的失效。

9.4.6.2.4 SIS 操作员接口的设计应能防止改变 SIS 应用程序。

9.4.6.2.5 在需要将信息从 BPCS 传输给 SIS 时，应使用系统、设备或程序来确认传输了正确的信息，并且不会损害 SIS 的安全完整性。

9.4.6.2.6 对于SIS操作员接口与BPCS操作员接口共用的情况，应保证从BPCS到SIS的不正确信息或数据不会损害安全性。

9.4.6.3 维护/工程接口要求

9.4.6.3.1 SIS维护/工程接口的设计应确保此接口的任何失效都不会对SIS执行AOPS的能力产生不利影响。这可能要求在SIS正常运行时断开维护/工程接口，如编程面板。

9.4.6.3.2 维护/工程接口应提供下列功能(同时为各功能提供访问安全防护)：

——SIS操作模式、程序、数据、屏蔽报警通信的方法、测试、旁路、维护；

——SIS诊断、表决和故障处理服务；

——增加、删除或修改应用程序；

——SIS故障检修的必要数据；

——在需要设置旁路时，旁路的设置应使得报警功能和手动停车装置继续有效(仅自动停车功能被旁路)。

9.4.6.3.3 维护/工程接口不应用作操作员接口。

9.4.6.3.4 启用和禁止"读-写"访问功能应仅能通过组态管理流程来实现，使用具有适当文档和安全防护(如授权和用户安全通道)的维护/工程接口。

9.4.6.4 通信接口要求

9.4.6.4.1 SIS通信接口的设计应确保通信接口的任何失效不会对AOPS使过程达到或保持某个安全状态的能力产生不利影响。

9.4.6.4.2 当SIS能够与BPCS和外部设备进行通信时，通信接口、BPCS或外部设备不应对AOPS产生不利影响。

9.4.6.4.3 通信接口应足够健壮以确保能承受电源电涌在内的电磁干扰而不会引起AOPS的危险失效。

9.4.6.4.4 通信接口应适用于不同零电位设备间的通信。

注：可能需要替代媒介(如光纤)。

9.4.7 AOPS随机硬件失效的定量

9.4.7.1 AOPS的失效量应等于或小于安全要求规格书中所规定的SIL对应目标失效量。这应由计算决定。

9.4.7.2 计算AOPS随机硬件的失效量应符合GB/T 21109.1—2007中11.9的要求。

9.4.7.3 量化随机硬件失效的影响时使用的可靠性数据应可信、可追溯、有资料支持且经过证实。

注1：可靠性数据要基于类似设备被应用于类似操作环境下所产生的现场反馈。包括：用户收集的数据，厂商/供应商/用户数据(从设备上收集到的数据的派生数据)，一般现场反馈的可靠性数据库中的数据等。在某些情况下，工程判断能用于评估缺失的可靠性数据，或估算对不同操作环境下收集到的可靠性数据的影响。

注2：缺乏能反映操作环境的可靠性数据是概率计算时经常出现的问题。终端用户要参照IEC 60300-3-2或ISO 14224要求组织相关设备可靠性数据收集。

注3：基于返厂的供应商数据需被限制在完全了解操作环境并完全参照IEC 60300-3-2或ISO 14224进行记录的设备种群。用户也可以记录AOPS的操作环境，并可证明供应商的操作环境数据与AOPS应用的环境匹配。

9.4.7.4 对于某个特定设计，如果未能达到相关AOPS的目标失效量，则：

a) 识别对失效量贡献最大的设备或者参数；

注1：可以使用故障树的割集分析。

b) 评估可能的改进措施对识别出的设备或参数的影响；

注2：典型的改进措施包括：选用更可靠的设备，增加针对共模失效的防护，增加诊断或检验测试覆盖率，增加冗余，缩短检验测试间隔等。

c) 计算实施改进措施后能实现的失效量；

d) 对比新失效量与目标失效量，并重复步骤a)～步骤d)直至以保守的方式达到目标失效量。

9.5 储罐防溢系统的安全防护设计

9.5.1 储罐防溢系统的设计应针对识别出的安全防护风险提供必要的弹性。

9.5.2 应开展安全防护风险评估以确认自动储罐防溢系统的安全防护漏洞，评估内容应包括：

——本次风险评估所覆盖的设备的描述(如 SIS、BPCS 或任何其他与 SIS 连接的装置)；

——识别出的威胁描述，这些危险可能利用漏洞并造成安全防护事件(包括对硬件、应用程序和相关软件的蓄意攻击，以及人为误差导致的非蓄意事件)；

——安全防护事件导致的潜在后果以及这些事件发生的可能性的描述；

——设计、安装、调试、运行和维护等各阶段对于安全防护的考虑；

——额外风险降低要求的确定；

——减少或消除威胁所采取的措施相关信息的描述或引用。

注 1：安全防护风险评估所需的边界条件信息和控制通常与设施的业主/运营公司有关，与供应商无关。这种情况下，设置的业主/运营公司有责任遵守本条。

注 2：SIS 安全防护评估可能被包括于整体过程自动化安全防护风险评估中。

注 3：SIS 安全防护评估对象范围可以从单个的 SIF 到公司内的所有 SIS。

10 储罐防溢系统安装要求

10.1 液位仪表的类型及材质选择应关注被测介质的下列特性：

——压力、温度、腐蚀性、导电性；

——是否存在粘稠、沉淀、结晶、结膜、气化、起泡等物理现象；

——密度和密度变化；

——被测液体中悬浮物的含量；

——液位扰动的程度。

10.2 当单台就地液位计无法覆盖整个液位范围时，可以选用多台仪表。多级液位计的重叠区应不大于 50 mm。

10.3 液位检测仪表安装要求按 GB 50093 的规定执行，安装位置和方式宜符合附录 A 的要求。

10.4 液位计安装设计时，还应满足液位计的检定和维修需求。

10.5 容量大于 100 m^3 的储罐应设液位测量远传仪表。储罐高液位报警的设定高度应按照第 9 章的要求执行。储罐低液位报警的设定高度宜满足泵不发生汽蚀的要求。外浮顶储罐和内浮顶储罐的低液位报警设定高度(距罐底板)宜高于浮顶落底高度 0.2 m 及以上。

10.6 安装在大型固定顶罐、浮顶罐的液位计宜安装在靠近扶梯平台的量油管内。

10.7 安装在罐侧面的液位开关，高高、低低液位开关宜在罐同一个方位角，其安装位置宜靠近罐盘梯处，但不应与盘梯接触。

10.8 安装在大型内浮顶罐的磁致伸缩液位计导向装置穿过内浮盘时，应加设密封。

10.9 在立式圆筒形钢制焊接储罐物料进出口管道靠近罐体处应设一个切断阀。

——储罐容量大于或等于 10 000 m^3，应采用气动型、液压型或电动型执行机构的阀门。

——储罐容量小于 10 000 m^3，可采用气动型、液压型或电动型执行机构的阀门。

——执行机构电源电缆、信号电缆应采用耐火型电缆。

——执行机构应设置防火保护。

——带有执行机构的切断阀应具有进料紧急停止功能。

注：紧急停止功能要包括自动、手动两种控制模式。

11 储罐防溢系统运行前安全确认要求

11.1 安装确认要求

安装前应确认：

——安全、操作、维护和紧急规程都已编制完成；
——确认计划编制是合适的并已完成确认活动；
——人员培训已完成，相应信息已提供给维护和操作人员；
——实现储罐防溢系统运行前评估的计划或策略已经就位。

针对安装，还应确认：
——是否有关于材料、工作质量、检验和测试的说明和规程；
——是否有监督以确保安装期间能够按照说明和规程正确执行；
——是否有预期的安装条件，当安装环境不满足预期条件时，是否有足够的防护措施；
——安装活动是否与其他工程活动有交叉，如果有是否有足够的防护措施来保证安装的质量；
——安装人员与监督人员是否有充分的独立性；
——是否保存了必要的检验记录；
——安装和检验规程在细节上是否足够清楚，以便使安装人员不用自己做出重要决策和解释；
——是否遵守了设计的保护、隔离和其他特殊要求；
——对于设计的变更是否有相关规程和说明。

11.2 硬件确认要求

针对硬件，应确认：
——硬件是否具有满足设计规格书和 SRS 要求的证明文件；
——硬件运行条件是否满足储罐防溢系统物理运行环境的要求：
- 温度范围；
- 湿度范围；
- 振动和冲击；
- 污染气体；
- 粉尘；

——是否采取了保护储罐防溢系统环境抗电磁干扰的预防措施，应包括以下方面：
- 储罐防溢系统的内在设计；
- 实际安装(例如，把电源和信号电缆分离)；
- 保护所有的输入和输出，避免输入电缆感应所产生的电压峰值的损害；
- EMC 测试规程；

——是否定义了关于设备之间的通信协议；
——储罐防溢系统界面在数据显示、报警等方面是否进行了定义；
——储罐防溢系统界面是否独立于 BPCS 界面。如果不独立，当 BPCS 有变更时，是否有措施可以避免不期望的储罐防溢系统逻辑变更。

11.3 功能确认要求

针对功能应确认：
——是否有关于储罐防溢系统全部功能的相关说明或规程；
——在功能确认的测试期间，是否有监督以确保说明和规程的实施；
——测试规程在细节上是否足够清楚，以便参与功能测试的相关人员不用自己作出重要方面的决策或解释；
——测试记录是否保存；
——如果开展在线功能测试，规程是否能确保该测试的安全实施；
——测试实施和相关参与人员是否进行了适合于他们的培训。

对于有 SIL 要求的 AOPS，除上述要求外，还应确认：
——是否有相关规程可用于对 SRS 中所定义的 SIF 进行功能测试；
——测试是否涵盖了 SRS 中所定义的 SIF。

11.4 应用程序确认要求

针对应用程序应确认：

——是否有关于应用程序测试的相关标准和规程；

——是否有监督以确保标准和规程的实施；

——关于说明、设计方面存在的缺陷或在应用程序期间发现的缺陷，是否有制定或修正规程；

——对设计规格书和 SRS 的偏差，是否有备案文件证明；

——关于设计规格书和 SRS 的更改是否经过变更管理审核；

——应用程序的测试是否由负责说明、设计和开发的相关人员参与和审核；

——是否对最终测试文档进行审核，以确保所有的设计规格书和 SRS 要求都已经过测试且符合设计。

11.5 操作运行确认要求

针对操作运行应确认：

——是否针对防止越权访问系统制定了合适的规程；

——操作说明和规程是否有文档记录；

——是否有合格的用户/操作手册；

——用户/操作手册中是否描述了可能的失效相关的风险以及针对失效的必要措施；

——执行操作任务的人员和所涉及的相关人员是否接受了相关的培训；

——是否有管理规程，以确保操作规程充分贯穿整个储罐防溢系统使用过程；

——对于设计中给出的假设条件，在操作和维护规程中是否有说明。

12 储罐防溢系统的验收要求

储罐防溢系统的功能安全验收活动可参考 GB/T 32203 执行。

13 储罐防溢系统检验测试和维护要求

13.1 一般要求

13.1.1 应制定书面规程，对储罐防溢系统硬件及程序进行测试、检查和维护，规程内容和活动频率应符合安全要求规格书或产品规格书要求，并考虑制造商建议。

13.1.2 储罐防溢系统的测试、检查和维护记录应至少保存三年。

13.1.3 应定期对储罐防溢系统组成部件进行目视检查，以确保没有未经授权的修改和肉眼可见的缺损(例如，螺栓或仪表罩缺失、支架生锈、线材开路、导管破损、伴热损坏和绝缘缺失)。

13.1.4 当现场工况(包括但不限于储罐操作、储存介质)、储罐及附件、仪表、系统发生变化时，应开展变更管理，对测试、检查和维护规程进行审查修改。

13.2 技术要求

13.2.1 检验测试应包括硬件测试和功能测试。

13.2.2 应对储罐防溢系统的所有部件定期开展检验测试，并形成文档记录，部件包括传感器、逻辑控制器、执行阀门等，还应包括 AOPS 其他组件，如涉及的安全栅、继电器等(如果有)。检验测试应每年开展一次，除非计算表明可选择其他检验测试频率(如要求时失效概率的计算)。

13.2.3 在检验测试中发现的任何缺陷，应安全地、及时地予以修复。修复完成后应再次进行检验测试。

13.2.4 对于具有 SIL 要求的 AOPS，应根据 SRS 安排检验测试。AOPS 在运行环境中安装后，检验测试频率应通过 PFDavg/PFH 计算来确定。

注 1：SIS 的不同部分可能要求不同的测试间隔，例如，逻辑控制器的测试间隔可能与传感器或最终元件的不同。

注 2：在运行一段时间后，根据现场因素重新评估并调整检验测试频率，典型因素包括：历史测试数据、工厂经验、硬件降级和软件可靠性等。

13.2.5 在预定的储罐大修时间间隔大于检验测试间隔的情况下，应设置在线测试/旁路设施。

——应符合安全要求规格书所定义的维护和测试要求。

——储罐防溢系统任何部分的旁路都应通过报警和/或操作规程对操作员发出警告。

——应编制操作规程，要求在由于旁路导致 SIS 被禁用或降级时，应在相应的操作限制下（持续时间、过程参数等）采取足够的风险降低补偿措施以维持安全。规程内容应包括旁路前、旁路中和旁路移除前操作员应完成的操作内容，以及允许在旁路状态下的最长时间等信息。

13.2.6 检验测试规程应涵盖所有储罐防溢系统（包括 LAH、LAHH、AOPS）组件，如传感器、逻辑控制器和最终执行元件，以及与储罐防溢系统相关的设施，如通信、报警诊断或断电报警等。规程内容应包括：

——制造商给出的维护模式下进行验证测试的方法，和测试完成后返回到工作模式的说明；

——为揭露 AOPS 未被诊断检测到的危险失效，需要执行的每个步骤：

- 每个传感器和最终元件的正确操作；
- 正确的逻辑动作；
- 正确的报警和指示；

——任何其他要求，如阀门关闭时间（阀门关闭时间和水击危害）。

13.2.7 如果对储罐防溢系统的任何组件或系统进行了更改，应立即开展检验测试进行验证。

13.2.8 检验测试应尽可能真实地模拟实际的高液位情况，但不应要求将储罐充装至 MW 以上。

13.2.9 在要求的检验测试间隔内应对储罐防溢系统回路中所有组件完成检验测试，包括传感器、逻辑控制器和最终元件（如关断阀和电机）。测试可为端到端形式，也将 AOPS 功能回路可分几部分进行。

13.2.10 针对储罐高液位传感器，可采用浸湿探头的方式开展测试（如使用实液或水来触发传感器，从而提供报警或 LAHH/AOPS 的功能激活）。

注：对于装有危险液体的储罐进行上述测试是不可行或不安全的。需编制技术说明文件，说明如何将传感器的完整性保持在适当水平。

13.2.11 应用程序测试应随 AOPS 功能测试一起开展。

13.2.12 对应用程序的任何变更都需要对受影响的 SIF 进行全面的确认和检验测试。如果对变更进行了适当的审查和部分测试，以确保变更是根据更新后的安全要求设计并正确实施的，则允许例外。

14 储罐防溢系统的变更管理要求

14.1 一般要求

储罐防溢系统变更管理应包括：

——硬件的变更；

——软件的变更；

——管理的变更；

——操作应用环境的变更等。

14.2 变更管理要求

14.2.1 在对储罐防溢系统进行任何变更之前，应建立授权和控制变更的程序。程序应包括明确的方法来确定和要求所要做的工作以及可能受到影响的危险（如储罐溢流风险）。

14.2.2 在对储罐防溢系统（包括应用程序）进行任何变更之前，应进行分析，以确定拟进行的变更对安全的影响。当分析表明拟进行的变更可能影响安全时，则应返回安全生命周期的第一个受影响的阶段。

14.2.3 应为变更和重新验证提供安全计划，变更和重新验证应按照该计划进行。

14.2.4 受变更影响的所有文档均应进行更新。

14.2.5 对于有 SIL 要求的 AOPS，应在完成功能安全评估并经过授权后，才能开始变更活动。

14.3 变更的文档要求

储罐防溢系统的修改或变更活动应形成文档记录，内容包括：

——修改或变更的详细描述；

——变更原因；

——修改活动对整个系统包括硬件、软件、人员因素、环境和可能的相互作用的影响分析；

——变更所要求的所有审批；

——变更活动的详细信息(如变更日志)；

——用于验证变更已正确实施的，子系统和组件的测试用例，包括重新确认数据；

——用于验证变更没有对储罐防溢系统未修改部分产生不利影响的测试，储罐防溢系统配置管理的历史(包括传感、阀门、控制等所有会影响储罐防溢系统执行的设备)；

——与正常运行和条件的偏差；

——系统规程的必要变更；

——文档的必要变更。

15 储罐防溢系统的停用要求

15.1 在对储罐防溢系统实施停用之前，应按照变更管理程序对停用计划和方案进行审查和控制，并按照管理权限进行审批。

15.2 停用计划和方案应包括储罐防溢系统停用的具体实施方法以及辨识可能导致的危险。

15.3 对拟停用的装置进行风险影响分析，包括对危险和风险评估进行审查或者必要的更新。评估也要考虑停用活动期间的功能安全，以及停用对相邻单元的影响。

15.4 评估的结果将用作制定下一步安全计划，包括重新确认和验证等行动的基础。

15.5 没有适当的文档支撑和审批授权，不应开展停用活动。

附 录 A
（资料性）
液位检测仪表安装要求

液位检测仪表安装要求如表 A.1 所示。

表 A.1 液位检测仪表安装要求

液位仪表名称	安装位置		安装形式
	顶部	侧面	
浮球式液位计	是	—	法兰式
浮筒式液位计	是	—	法兰式
钢带浮子液位计	是	—	法兰式
磁浮子液位计	是	是	法兰式
磁致伸缩液位计[a]	是	是	法兰式
伺服液位计	是	—	法兰式
雷达液位计	是	—	法兰式
射频导纳式液位计	是	—	法兰式
静压式液位计	—	是	法兰式
音叉液位开关	是	是	法兰式
超声液位开关	—	是	外贴式
[a] 当侧面安装磁致伸缩液位计时，采用磁致伸缩液位计可与磁浮子液位计组合安装形式。			

参 考 文 献

[1] GB 17681—1999 易燃易爆罐区安全监控预警系统验收技术要求

[2] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语

[3] GB/T 32202 油气管道安全仪表系统的功能安全评估规范

[4] GB/T 32203 油气管道安全仪表系统的功能安全验收规范

[5] GB 50074—2014 石油库设计规范

[6] GB 50253—2014 输油管道工程设计规范

[7] GB 50737—2011 石油储备库设计规范

[8] AQ/T 3034—2010 化工企业工艺安全管理实施导则

[9] AQ 3035—2010 危险化学品重大危险源安全监控通用技术规范

[10] AQ 3036—2010 危险化学品重大危险源罐区现场安全监控装备设置规范

[11] SH/T 3007—2014 石油化工储运系统罐区设计规范

[12] ISO 14224:2017 Petroleum, petrochemical and natural gas industries—Collection and exchange of reliability and maintenance data for equipment

[13] IEC 60300-3-2:2004 Dependability management—Part3-2:Application guide—Collection of dependability data from the field

[14] IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

[15] API PR 2350:2012 Overfill Prevention for Storage Tanks in Petroleum Facilities