ICS 71.040.10
CCS N 53

中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX/IEC TR 63176:2019

`

安全仪表系统(SIS)—过程分析技术(PAT)系统

Process analysis technology systemes
as part of safty instrumented systems

IEC TR 63176:2019,IDT

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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

引　言

本文件用于帮助过程分析仪技术的用户，按照安全仪表系统(SIS)要求安装使用设备。本文件中可能涉及有安全相关的约束性条款的内容，但整体文件内容是推荐性。例如，过程分析技术(PAT)作为测量设备，在过程工业中被用作安全仪表系统(SIS)的传感器组件，在大多数情况下，他们代表了监控过程变量的唯一或最有效的方法，就其本身而言，可以对设计的保护系统的使用进行可靠的评估。由于与过程介质的直接接触材料的相互作用，过程分析技术(PAT)测量设备比广泛使用的压力、温度、灌装液位和流量测量的传感器通常更容易发生故障，需要更多的维护。这种相互作用将导致无法完全避免的系统性失效，可通过短时间内定期检查测量设备来解决此问题发生。

过程分析测量变量和方法的多样性，在每种情况下受信号、准确度限制，应用的过程分析技术(PAT)测量设备的数量相对有限，因此大多数情况下难以按照IEC 61511进行功能安全性的定量评估。除作为安全仪表系统(SIS)组件性能评估欠缺外，相似的应用数量也太少。然而，在过去的30年里，过程分析仪企业已成功把数百个安全仪表系统(SIS)应用到过程分析技术(PAT)测量设备的之中。

在无法满足规范要求或只提出部分措施的领域，这些措施在谨慎应用时才可达到同等的安全水平。

关于电气和电子系统功能安全相关的要求在IEC 61508中有描述，在IEC 61511中规定了“过程工业中的安全仪表系统(SIS)”。本文件描述了过程分析技术(PAT)测量设备作为安全仪表系统(SIS)一部分的程序指引。

安全仪表系统(SIS)—过程分析技术(PAT)系统

1 范围

本文件适用于过程工业安全仪表系统(SIS)中过程分析技术(PAT)测量装备的规划，安装和运行（维护）。它涵盖了安全设备认证的所有必要步骤，并通过附加对过程分析技术(PAT)设备的特殊要求来补充安全仪表系统(SIS)设备的安全管理。

本文件不涉及整个的安全仪表系统(SIS)设备的安全管理。

本文件使用的术语“认证”专指过程分析技术(PAT)系统用于安全仪表系统(SIS)设备的适用性测试，与制药环境中使用的术语“认证”不同。

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。

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本文件。

3.1 术语和定义

3.1.1

过程分析技术(PAT)测量设备 PAT measuring equipment

用于实现相关物质测量功能所必要的设备和介质的总和。

注：包括但不限于取样设备、样品输送设备、样品处理设备、样品回收设备、分析仪、PAT控制单元和基础设施，如给料、参比和校准以及必要的供电电源。根据具体情况下，还应有仪表柜或放置分析小屋或站房。

3.1.2

基本测试 basic testing

为安全仪表系统(SIS)预先选择合适的分析设备，不需要参考特定的测量任务。

注：只适用于附录A中提及的特定指标的分析设备的测试。

3.1.3

应用测试 application testing

确保测量目标可以被PAT系统成功实现的测试。

注：包括检查配置、有时需要根据相应测量方法对分析设备进行编程，以及考虑样品处理产生的影响，特别是准确度、确定组成（背景组分）、状态变量的影响（压力，温度，流量）、介质和分析设备环境影响以及稳定性。

3.1.4

操作经验 operational experience

在使用分析仪之前具备的仪器知识，包括用于类似测量方法所需配件的知识。

注：仅涉及通过相似分析设备用于类似测量任务而获得的实际使用经验。

3.1.5 **运行中的测试 in-service testing**

在生产运行期间，监控安全仪表系统(SIS)中的PAT系统的运行。

注1：在此可明确验证过程分析技术(PAT)系统的操作性能程序与相应安全仪表系统(SIS)设备程序之间的明显差异。

注2：记录将要进行的测试工作，时间表以及在运行中的测试期间不同情况下满足安全功能所需的额外措施及该阶段的负责人员结果评价形成的规范。

3.1.6

性能认证 proven performance

指过程分析仪安装是否适合作为安全仪表系统(SIS)的一部分做出最终判定的全部认知。

注1：通过大量的运行经验，包括对测量任务适用性获得确认，如果不行，可通过运行中的测试得到性能认证。

注2：由专家团队最终确定过程分析技术(PAT)系统性能认证，其确定方式与通常用于现场设备和PLCs的方法不同。

3.1.7

校准 calibration

检验工作，确认目标状态。

注1：“校准”是指确定并记录测量值与真值（参考值）的偏差。

注2：在校准过程分析仪时，在规定条件下确定并记录输入和输出之间的关系，输入值是被测物理量，输出值是测量装置的电气输出信号。

3.1.8

调校 adjustment

为了消除系统误差而对分析仪进行的设定或修正，直到满足预期应用的要求。

注：调校是通过设定或调节仪表使得测量误差尽可能小以接近额定值，达到装置规范值内。这种调校是永久改变仪器的过程。

3.1.9

测试间隔 test interval

过程分析技术(PAT)系统作为安全系统的一部分，对不同等级的检验测试有不同的试验间隔。

注：测试间隔有下列几种情况：

——有内置在过程分析技术(PAT)系统的诊断传感器（像流量计）；

——有内置在过程分析技术(PAT)系统的通道（像自动校准通道）；

——有内置在过程分析技术(PAT)系统的通道（像自检和手动调试；维护）；

——有整个系统的（像手动，过程分析技术(PAT)+安全仪表系统(SIS)其他部分测试）。

3.1.10

检验测试 proof testing

在技术安全系统中进行检测以发现错误，必要时，可让系统恢复到满足其需要的功能状态。

3.1.11

检验试验范围 proof test coverage

3.2

在技术安全系统中发现错误的测试覆盖率。

注：该术语最初归类于检验测试。然而，原则上任何测试（见测试间隔）不可能完全覆盖。对于传感器，该通道未能发现危险故障比率（DU）会因为丧失功能而增加，而能发现危险故障比率（DD）会降低。自动校准通常仅在足够短的时间间隔内检查一定的未发现危险故障率(DU)，也不排除在经过核查和维护后仍未发现该通道故障。需要仔细做一份测试过程的详细计划确保尽可能不发生这种情况。

符号和缩略语

下列符号和缩略语适用于本文件。

DC： 诊断覆盖率 （diagnostic coverage）

DD： 能检测到的危险 （dangerous detected）
DU： 不能检测到的危险 （dangerous undetected）
FAT： 工厂验收测试 （factory acceptance test）
FMEA： 故障模式和影响分析 （failure mode and effects analysis）
FMEDA： 故障模式，影响和诊断分析 （ failure mode, effects and diagnostic analysis）
HazOp： 危害性和可操作性研究 （hazard and operability study）
HFT：硬件故障裕度 （hardware fault tolerance）
PAT：过程分析技术(PAT) （process analyser technology）
PFD： 要求的失效概率 （ probability of failure on demand）
PID： 管道和仪表图 （piping and instrumentation diagram）
SAT： 现场验收测试 （site acceptance test）
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(SIS) （safety instrumented system）
SFF： 安全失效分数 （safe failure fraction）
PTC： 检验测试覆盖率 （proof test coverage）
λ_i：第i组件的失效性
μ_i：第i组件的修复率
$U_{DD,\ i}$：第i组件由DD失效导致的不可用性
$U_{DU,\ i}$：第i组件由DU失效导致的不可用性
U_{ch1}：通道1不可用性
U_{MOON}：整个系统在MOON配置的不可用性
β：共因失效的比例
T_{Max}：最大测试间隔
PFD_{Deta}:由于共因失效所占的PFD比例
PFD_{MOON}：不考虑共因失效下的PFD值
PFD_{PAT}：整个过程分析技术(PAT)系统的PFD值

4.1 4 审核程序

概述

PAT测量设备通常是复杂的安全仪表系统(SIS)传感器，需单独定制（设计）以适应过程工艺的特定要求，其功能是通过一种或者多种物质浓度的测量来反应工艺过程状况。

这些传感器的独有性能通常不像现有SIS有足够数量的操作经验引入到新规划使用的PAT测量设备中。在这种情况下，对完整功能的测量设备开展运行中的测试。这些测量设备的独有特征要求参与整个过程中各种认证过程该部分的（人员具有）高水平的技术能力，并在工艺中有各个层次的鉴定过程描述（参见图1）。这包括过程分析技术(PAT)系统的（安装）工程人员和操作人员（见4.2和4.3），并记录每个审核步骤。

认证过程由过程分析技术(PAT)专家执行，同时有工艺控制和工艺过程设计的安全工程师的参与。所有与过程分析技术(PAT)系统性能相关的过程数据应由负责安全的工程师确认。

当几种测量方法都是技术可行的，应对这些方法进行考查和评估。从计划一开始就应考虑进一步减少/最小化过程分析技术(PAT)系统整体失效概率的问题，包括：

——冗余程度/故障容错程度；
——同质或多样性冗余；
——其他测量装备的操作经验/已证明的性能；
——与计量应用相关的风险（比如交叉灵敏度干扰，老化过程，共因失效）。

计量适应性可从早期应用的经验中确定，或在应用测试的环境中被证明。

当使用冗余系统时，应考虑监测测量值的偏差。

测量方法选择后，确定样品处理的设计和相关部件，部件的设计和选型都要进行功能性论证并归档。应使用合适的和可靠的设备与部件来搭建过程分析技术(PAT)测量系统。可靠性的验证通常基于操作人员的操作经验，也可由制造商进行的可靠性评估实现。

对于特定应用的技术规范（比如，失效率、检验测试间隔等），安装工程人员和/或工厂操作人员比制造商有优先权，可以不考虑制造商的建议来负责对SIL进行分级以适用于应用。虽然应优先使用经过SIL认证的分析仪，但这并不意味着强制使用经制造商SIL认证的分析仪。因此，相对于经SIL认证的分析仪，也可以优先使用未经SIL认证的分析仪。

分析仪能够实现的应用也没有必要只局限于由特定制造商认可的应用。例如，如果完成了鉴定程序，虽然制造商认证为SIL1，而已得到性能证明的分析仪就没有理由不可以用于单通道SIL2的应用。

对于过程分析技术(PAT)测量设备，应对整个过程分析技术(PAT)系统进行详细检查。目的是检测潜在的失效，评估这些失效对功能安全的影响。由此可提出失效控制、失效避免、故障检测或降低失效频率的相应措施。应估算PFD值，在4.5.6中提到了估算要求选项。PAT的PFD值需要在安全仪表系统(SIS)的整体PFD值估算中加以考虑。

在认证性能时、合格的HFT值(见4.5.5)和PFD值(见4.5.7)可用的情况下，过程分析技术(PAT)系统对安全仪表系统(SIS)的适用性应作为最终衡量标准进行考虑。

由于过程分析仪设备的复杂性，SFF是不充分的。因此，没有对SFF开展评估，也没有做为过程分析技术(PAT)系统的指标。

如果没有足够的数据来支持认证性能，但是测量方法已经成功用于类似的应用中，过程分析技术(PAT)系统作为安全仪表系统(SIS)的安全装置的适用性，可通过实时运行过程的运行中测试记录(见4.5.8)来确定。

做为运行中测试过程的结果，操作人员可能会遇到需要满足维护功能安全的要求。最终，过程分析技术(PAT)测量设备的生命周期应该从试运行到停运全程被记录存档下来。

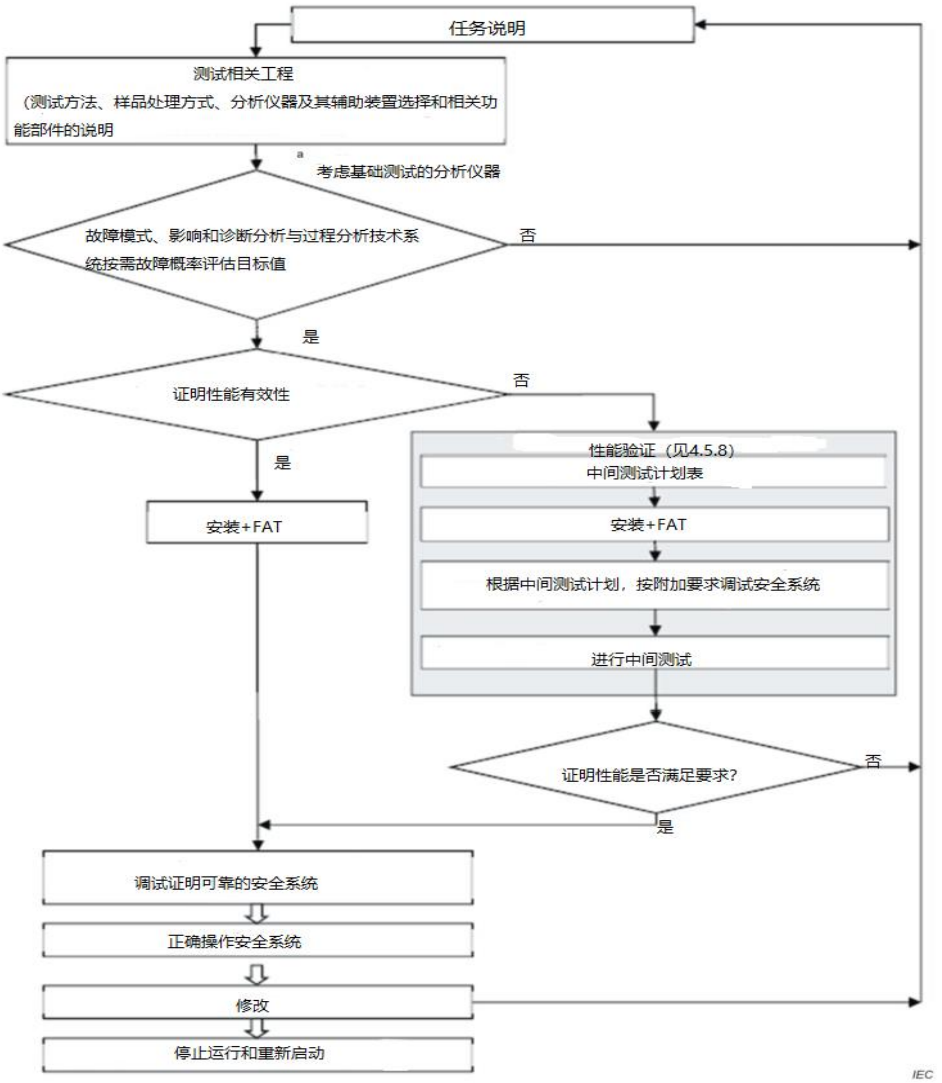


图1 PAT 测量系统认证过程层级

对安装工程人员要求的建议

4.2 下面要求来自于IEC 61511 -1: 2016中5.2，详细阐述了过程分析技术(PAT)处理措施。作为安全仪表系统(SIS)一部分的过程分析技术(PAT)装置的安装核查需要对过程分析技术(PAT)领域及其在化学和/或物理应用领域有丰富的知识和经验，可由专家团队把这些知识和经验总结用于指导资格认证工作。参与实施的生命周期的安全的人员、部门或组织应当有能力完成其所负责的任务。负责审核过程的人员需要对各自的任务具备足够的管理和领导素质，并知道可能发生的任何事件的后果。只有在团队能够清楚评估安全各方面问题后，才能应用新的和复杂的应用或技术。

专家团队应具备下列知识和经验：

——在测量现场与化学或物理过程步骤相关的知识；

用已知的测量现场的物理和/或化学特性参数评估分析仪在化学或物理过程中的可用性(即评估分析仪对某个应用中的适用性)。在正确操作的整个范围内考虑(可接受范围和允许故障率范围)，直到出现操作不正常的限值。启动和停运应与正常生产操作一样加以考虑，是否安全功能被明确免除。

——分析仪的应用准备经验；

从物理和化学的角度理解某种测量方法及其限值是安全仪表系统(SIS)中准备使用的分析方法所必需的。

——样品处理过程的设计经验；

样品处理过程的系统组成、样品处理过程的工程设计、样品的物理和化学性质以及测量过程的知识是评估样品处理过程适用性所必要的。

——安全工程设计工作方法的知识；

有能力进行故障模式、影响和诊断分析(FMEDA) ，评估过程分析技术(PAT)系统的失效概率值(PFD)，并有能力配合进行风险分析（比如利用危害性和可操作性研究方法(HazOp)，用于预知，事故原因审核，效能评估和对策）是必要的。

——应用的法典和标准的知识：

4.3 本文件涉及到设计的相关法规和标准参见IEC 61508和IEC 61511。

岗位操作人员的要求的建议

参见IEC 61511 -1: 2016,6.2，具体规定了过程分析技术(PAT)事项。按照过程安全仪表系统(SIS)安装的过程分析技术(PAT)的操作人员应确保在整个生命周期中，在运行和维护期间，所涉及的安全功能的安全完整性达到所需的SIL水平。如果安全仪表系统(SIS)需保持功能安全性方式运行和维护，就应能提供与维护等级相适应的能力，或将维护工作委托给具有相应能力的服务提供商。组织形式不限定。

除了IEC 61511规定的要求外，还应具备下面的知识、技能和经验：

——过程分析技术(PAT)系统功能性的知识；

4.4 过程分析技术(PAT)系统的校准功能的知识，特别是样品预处理，理解测量方法的基本原理，通常由环境条件和与测量介质的相互作用影响测量系统功能极限的知识。

——过程分析技术(PAT)设备维护的技能和经验；

熟悉过程分析技术(PAT)测量系统的机械和电气工作，包括维修和维护工作，有识别故障的经验(例如，测量系统的偶发故障，不能正常工作)。

基本测试（仅限分析仪）

4.5 安全系统中使用的每一台分析仪都应满足基本质量要求。基本(本段所有都改)测试有助于检验这些质量要求(见附件A)。基础测试不能取代分析仪的应用测试，该应用测试将针对有关的样品处理系统或验证性能。

由于基本测试的结果是由分析仪的硬件和软件所决定，因此应确保制造商记录的硬件或软件的变更以及每项基础测试的更新。如果制造商开发的分析仪符合IEC 61508的质量要求，基础测试一般不需要更新。

工程设计

4.5.1 总则

作为安全仪表系统(SIS)一部分的过程分析技术(PAT)测量装置的安装设计应严谨,因为这对安全仪表系统(SIS)后续运行的有效性有决定性影响。

从根本上说，过程分析技术(PAT)系统的工程设计应基于包括所有物理和化学性质(压力、温度、成分、相态、露点等)的工艺数据的技术参数表。

过程分析技术(PAT)系统结构通常比其他测量系统（如压力、温度或流量）更加复杂。特别是在线测量系统，该系统在生产过程中移取混合物中的代表性组分，并对其进行条件调整，以供后续分析。这可通过阀、泵、冷却器、分离器和过滤器等组件改变混合物的组成。同样，可能出现这样情况：样品不能再传送到分析仪，或传输速度不够快，测量值不符合实时数据的要求，因此，样品处理是安全仪表系统(SIS)不可分割的一部分，应在失效概率(PFD)测定过程中被考虑到。

在某些情况下,样品处理可严重影响过程分析技术(PAT)系统传感器安装的失效概率(PFD)值。为此，过程分析技术(PAT)系统装备了附加的传感器，可在尽可能短的时间内识别样品处理错误，降低现存的未检测到故障危险比例，转变为可测故障危险。

除了验证测试之外，与传统的安全系统相比，过程分析技术(PAT)系统还需要在更短的时间间隔内进行进一步的人工测试和校准，包括根据具体情况进行的必要调整。手动或自动校准，而不进行前述的手动测试间的调整，可有助于过程分析技术(PAT)系统的可行性测试。

附加传感器的校正功能决定了危险的不可测的故障和可测的故障之间的比例，因此，在适当的情况下，这些故障将在测试间隔中单独监测。

4.5.2 设计数据

安全仪表系统(SIS)一部分的过程分析技术(PAT)测量装置的设计基于以下原则：

——安全仪表功能(SIF)的定义

功能安全的性能水平（如：安全完整性水平(SIL)），这被认为是类似于安全评价/产品线的风险分析和记录，此目标是限制过程中的某特定条件参数。在过程分析技术(PAT)中，这通常涉及到某确定物质的浓度的上下限。

——安全系统的最大允许响应时间；

在过程分析技术(PAT)设计时应考虑到这一点,这与样品滞后时间(即样品采集、传输和分析周期)、驱动器和逻辑元器件的响应时间有关。

——取样点的过程设计数据。

这包括待分析样品的组成和取样点物料传输的物理/技术数据，包括毒性和腐蚀性。在此背景下，应考虑特殊系统条件(如启动、关闭、负载变化、故障)的影响。

4.5.3 带应用程序的分析仪

测量原理和分析仪的选择可根据设计数据，在选择分析仪时，应优先考虑附录A中已确定的通用分析仪。

具体的计量适用性可以通过现有的可比性的应用确定。然而通常在分析仪应用过程中进行验证。

选择测量方法和分析仪的原因记录下来。

4.5.4 样品处理

所需的样品处理取决于不同应用案例的工程设计数据和所选择的分析仪。

样品处理最好包含诊断功能，以便能识别出影响安全功能的故障并发出信号(避免未发现危险故障(DU)和将未发现危险故障(DU)转化为已发现危险故障(DD))。

在可能的情况下，外围应包含已验证运行可靠的组件。

（过程分析技术(PAT)测量装置)完整的系统由样品处理和分析仪组成,应在分析仪流程图(P&I图）中说明，并附有部件清单。

4.5.5 硬件容错率(HFT)

硬件容错率(HFT)提供有关于系统冗余程度的信息，参见IEC 61511-1: 2016, 11.4，表1中列出了硬件容错率:

表1 安全整体水平（SIL）中最小硬件容错率（HFT）要求

SIL	中间测试中最小硬件容错率	经充分验证性能后最小硬件容错率
1	0	0
2	1	0
3	2	1

性能验证对于安全仪表系统(SIS)中的过程分析技术(PAT)系统是必要的（见第4章），相应的选项基于早期的应用（IEC 61511-1:2016,11.5）。

在性能得到充分验证的情况下，只有在过程分析技术(PAT)系统中仅能配置与过程相关的参数并保护此设置时，才能用最小硬件容错率。性能验证期间编写的过程分析技术(PAT)系统或分析仪软件应解释说明和记录，并重新开始验证试验。

4.5.6 过程分析技术(PAT)系统的故障模式的影响及诊断分析(FMEDA)

应对整个过程分析技术(PAT)系统进行故障概率和影响分析，包括传输、比对和辅助介质(如FMEDA-故障模式、影响和诊断分析)。在此期间观察到的故障应进行描述并适当分类(如DD -已检测到危险，DU -未检测到危险，S -安全)，列出故障率(包括常见原因，常见模式)，并详细说明其来源(如制造商规范，自己的统计数据)。潜在故障由专家团队识别，并确定其故障率。识别出的故障应进一步按随机性和系统性进行分类。应尽可能对系统性故障进行补救，如果不行，系统故障应通过诊断设备来识别。过程分析技术(PAT)系统的定期检查应努力做到性能验证（验证测试）的覆盖率达到100%。如果估计验证测试覆盖率偏低，该保守的评估值应记录下来并给出合理解释。由于所涉及的估计不准确，对个别故障率的统计处理可能与实际不符，应遵守所有相关的正确操作条件。

故障模式、影响及诊断分析(FMEDA)的范围取决于过程分析技术(PAT)系统的复杂程度，附录B列举说明了这类容易出问题点的分析说明。

另一方面，通过有组织的测量来排除这种人为错误(如使用不合适的辅助介质)。同样地，通过其他合适的方式（如不断变换切换点），消除，在故障模式，影响和分析(FMEDA)中未考虑的系统性错误（如测试气体浓度不准确性）。

4.5.7 过程分析技术系统故障(PFD_{PAT})值的评估

过程分析技术系统故障率PFDPAT值的估算整个过程分析技术系统故障率(PFDPAT)值用于估计过程分析技术(PAT)测量系统要求的失效概率，仅代表安全系统的要求的失效概率(PFD)的一部分。在所有情况下，在整体评估中应考虑进一步的要求的失效概率(PFD)(如：逻辑或驱动器相关)。在某些情况下，可以通过附加状态信号(未发现危险故障(DU)转化为已发现危险故障(DD))和/或减少维护间隔来降低整个过程分析技术系统故障(PFDPAT)率。如果不行，测量系统应在必要时改变或增加通道的数量。整个过程分析技术系统故障(PFDPAT)率过高最终判别排除作为安全仪表系统(SIS)的测量装置。

过程分析技术系统故障(PFD_{PAT})率值应采用相应的过程确定。一种方法，数值离散方法以示例的方式如下说明。

基于系统分部件随时间t的失效性，利用电子表格分析，实现确定要求的失效概率(PFD)值的数值离散方法。与分部件相关的失效性会相应叠加，从而形成整个系统的失效性。要求的失效概率(PFD)值是通过在系统生命周期或发生在曲线进展的最长周期内平均失效性$U(t)$来确定的。

首先通过 (FMEDA)记录潜在故障，并将其分为安全S、检测到危险DD和未检测到危险DU，这些故障是形成失效性的基本条件。

部件失效性U（t）的公式普遍使用的，并构成IEC 61508-6中用于计算PFD值的公式的基础。

具体方法参见附录C。

4.5.8 验证性能-对过程分析技术(PAT)系统进行各种不同的中间测试

通过充分的操作经验，包括对测量任务的适宜性的认可，将获得可靠的性能。如果不可行，可以通过中间测试来验证性能。

完成材料流程图、零件清单和PFDPAT值估算后，应决定是否有可比性的PAT测量系统的足够操作经验。由上述专家组确定是否有足够的操作经验，或在适当的情况下要求对过程分析技术(PAT)测量系统进行中间测试，在所有操作条件下，在设定的测量位置进行。中间测试应在下述条件下进行:

——可预计完成后的中间测试有好的结果；

——预估过程分析技术故障率(PFD_{PAT})值足够低（即：由于逻辑的和执行器系统的参与仍保留了相当大的未发现故障率），如果在规划过程中已经假定实现了最大可能的 (PFD)值，则不应通过中间测试来证明性能；

——部分规划好的过程分析技术(PAT)部件应已经成功地使用在类似的位置；

——在中间测试阶段，安全功能应根据具体情况补充附加测量；

——在开始安装之前，应记录运行中的中间测试和评估标准，以便用于以后证实的性能的测定；

——如果最终无法验证已证实的性能，则应在必要时以另一种方式并通过过程分析技术(PAT)以外的方法来保证安全功能。这意味着过程分析技术(PAT)方法不适用这种情况

借助于中间测试，可确立新的分析仪或新的样品处理的安全功能。

4.5.9 过程分析技术(PAT)系统的安全逻辑

作为安全仪表系统(SIS)装置的一部分，过程分析技术(PAT)系统可有自己的逻辑单元，例如，便于测量点切换或预先连接信号单元。

原则上，逻辑器件可在主控制系统或上级安全相关的PLC或逻辑运算器中实现，置于单独的过程分析技术(PAT)控制器(PLC，安全相关的PLC或逻辑运算器)中，或完全集成在分析仪中，也可以是混合形式。

当与安全相关的信息被单独处理时，重要的是要遵循功能安全的标准和指南(例如，使用与安全相关的PLC)。

4.5.10 样品切换

额外的风险与测量点切换有关，在所有情况下都应将其视为误差来源。由于切换阀故障导致的未知危险故障(DU)可以通过位置指示器转换为已知危险故障(DD)。此外，还应考虑切换引起的与触发安全系统相关的极限值响应时间延长。

4.5.11 运行期间周期性检查计划的编制

整个测量系统的周期测试频率应在（PFD）值预估的背景下确定。理想情况下，这些定期测试应该识别所有潜在的未知危险故障（DU）和怠速监测装置，包括位置指示器、液位、流量、压力或温度限值传感器。

4.6 应估计周期性测试检测到所描述的故障的程度。在估算按需故障率（PFD）值时，应该考虑这个验证测试的覆盖范围。

4.7 测试间隔对按需故障概率（PFD）值有相当大的影响。

安全系统的调试

在有文件证明性能的情况下,调试在安装和现场验收测试(SAT)之后进行。如果没有经过性能验证，调试可与中间测试同时进行。运行和维护人员应进行培训。

审核过程的记录

审核过程的记录包含以下要点：

——运行/危险和可操作性研究(HazOp)的安全评价危害性摘要；

——工艺工程数据分析工作表；

——分析仪，技术参数表；

——物料流程图及零件清单（过程分析技术(PAT)流程图(P&I)，过程分析技术(PAT)工艺流程图(P&ID)）；
——分析仪/部件文件（如：安全完整性等级(SIL)证书）；
——预估按需故障(PFD)率，包括故障模式，影响和诊断分析(FMEDA)协议；
——安全仪表系统(SIS)回路示意图；
——功能图表；
——与测量功能相关的安全注意事项；
——测试规范；
——为操作人员编制的安全功能的信息；
——维护计划表；
——资质标志验证的负责人；
——列出专家组参与者姓名；
——分阶段中间测试的计划表和记录。

5 常规运行

总则

5.1 第5章提到的所有任务都应由安全系统的操作人员开始实施。

运行期间的周期性测试

5.2 4.5.7中确定的 (PFD)值直接取决于定义的测试间隔。因此，应遵守测试间隔，并将其记录在运维计划表中。

检验应记录在检测报告中。建议制定详细的检验程序计划，这可能取决于不同的运行阶段和实际情况(如：启动阶段测试)。

整个系统的检查:传感器-逻辑系统-执行器应与相关的其他任务进行协调和执行，参见IEC 61511 -1:2016中5.2.1~5.2.3。

5.3 安全系统的功能根据所涉及的任务定期进行验证，其中包含过程分析技术(PAT)系统。

运行中的文件和记录

5.3.1 总则

建议设备操作人员根据规定的计划表和管理条例保存记录，按计划和管理条例指引规划方式进行定期测试(见5.2)，参见IEC 61511。

这些记录至少应包含以下信息。

5.3.2 维护计划表

维护和检验计划(M+I计划表)表描述了在各个时间间隔内应执行的工作。M+I计划表至少包含以下信息:

——测量点编号，安全功能编号；
——测试间隔；
——适用的测试规范条款。

按需故障概率(PFD)值直接取决于4.5.7中测定的MTTR，故平均维护持续时间(MTTR)不能过长。

5.3.3 作业指导书

根据试验规范(见 4.7)进行的检验应在工作指导书中说明。

5.3.4 工作记录

在5.2中提及的测试报告至少包含以下内容：

——完成检验和维护工作的日期；
——参与检验和维护工作人员的姓名；
——已修复故障(类型)的说明；
——在多通道安全系统中标注出受影响的通道；
——清晰标识所测试的系统(如：测量点编号、安全功能编号)；
——测试间隔的偏差；
——适用的测试规范条款；
——系统在维护后且无任何故障下重新投入使用时的工作及验证的结果。

5.3.5 故障数据记录

每次运行维护都应做记录，包括样品处理在内的整个系统。5.3.4给出了需要记录文件的内容。
每次装置故障可按如下分类：
——故障位置（过程分析仪，样品处理）；
——故障检测（如：验证性能）；
——故障的性质（危险，安全）；
——故障的类型（随机的，系统的）；
——故障的原因（如：工艺过程，设计缺陷，装置故障，错误校准）；
——故障的细节（如：设备型号和制造商）。

5.4 故障数据估算和偏差处理

在持续改进过程的背景下，故障数据应在生产设备的操作人员和过程分析技术(PAT)专家之间进行评估，减小相对于正确操作的偏差。

5.5 修改

5.5.1 过程分析技术(PAT)系统的修改

修改安全系统后存在某些风险，比如系统性故障可能不经意地或者错误地被执行并损害该安全系统在需要的情况下的表现。在这种情况下，按需故障概率（PFD）值改变了，这意味着可能不再符合所需的安全完整性等级（SIL）分类标准。在修改评估时，应采用与规划和安装现有安全系统时相同的系统。应将修改内容通知相关的运行和维护人员，并在必要时就修改内容进行培训。
如果部件不能以1:1的比例替换相同的备件，这被视为修改，并将被检查，此情况适用于硬件和软件。制造商对安全系统部件进行软件和硬件的修改，制造商应给出报告。
如果软件开发依据IEC 61508，则可免除软件的更新测试。

5.5.2 过程工艺的修改

5.6

在对过程工艺(化学的和物理的)参数或所用材料进行修改时，应评估和记录其对安全适用性的影响。应采用与规划和安装现有安全系统相同的系统，并且原始文件由操作人员保管。

5.6 停止运行和重新启动

5.6.1 停止运行

停止运行是指停止供电和辅助电力。某一过程的断开不代表过程分析技术(PAT)系统的停止运行。

5.6.2 重新启动

重新启动相当于初次启动，如果运行正常没有改动，中间测试阶段可省略（见5.5.2）。

5.7 溯源性

一般应使用现有标准中的安全规则。如果发生变更，应考虑具体的过程分析仪的工程要求。

附 录 A

（资料性）

分析仪的基本试验项目

基本试验项目只涉及未来在安全设施中使用的分析仪的质量和操作特性的基本要求，其技术适用性取决于这些分析仪的技术适用性。通过与任务相关的应用测试，确保对特定测量任务的实际适用性。

基础试验项目内容

1 组织检查（Organization check）

1.1 类型/版本(Type/Version)

1.2 测量范围、传感器（Measurement range, sensor）

1.3 系列号（Serial no.）

1.4 硬件（Hardware rev. no.）

1.5 软件（Software rev. no.）

1.6 文档（Documentation）

1.6.1 文档版本号（Documentation version number）

1.6.2 理解程度（Comprehensibility）

1.6.3 正确性（Correctness）

1.6.4 完整性（Completeness）

1.6.5 用当地语言编写的操作和安全说明（Operating and safety instructions in the local language）

2 分析仪制造商规范（Manufacturer specifications on analyser）

2.1 开发参见IEC 61508 的SIL2或SIL3（Development pursuant to IEC 61 508 SIL2 or SIL3）

2.2 EMC参见IEC 61326-3-1/IEC 61326-3-2(EMC assured pursuant to IEC 61 326-3-1 / IEC 61 326-3-2

2.3 未发现故障率（Failure rate DU）

2.4 发现故障率（Failure rate DD）

2.5 Failure rate SU

2.6 Failure rate SD

2.7 测量功能的欧盟设计型式试验证书（EC design pattern test certificate for measuring function）

2.8 允许的湿度（Permissible humidity）

2.9 环境温度范围（Ambient temperature range）

2.10 环境温度影响Ambient temperature effect

2.11 过程温度范围（Process temperature range）

2.12 过程温度影响（Process temperature effect）

2.13 过程压力范围（Process pressure range）

2.14 过程压力影响（Process pressure effect）

2.15 振动影响（Effect of vibrations）

3 维护评估（Maintenance appraisal）

3.1 设计（Design）

3.2 职业安全（Occupational safety）

3.3 操作性（Operability）

3.4 重新设置为默认设置的能力（Capacity for resetting to default settings）

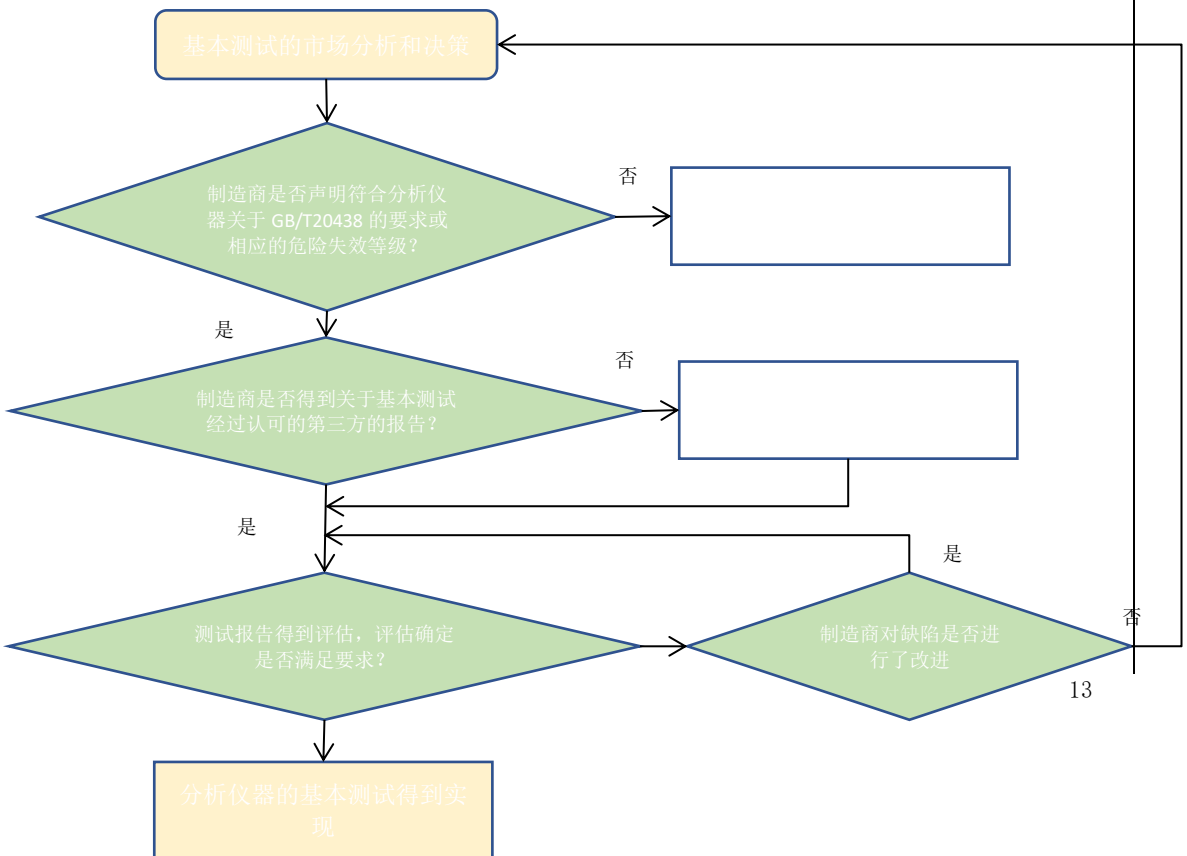
3.5 锁定参数（Locking of parameterizing）

3.6 故障信号（Failure signal）

3.7 服务请求信号（Service request signal）

3.8 服务信号（Service signal）
3.9 维护费用（Maintenance outlay）
3.1 0 维护友好（Maintenance friendliness）
3.1 1 接受对制造商设备的经验数据的评估（Experienced data about manufacturer's devices subject to this appraisal）
4 防爆评估（Explosion protection appraisal）
4.1 与其他装置互联能力（Interlinking capability with other Ex-devices）
4.2 检验证书/操作手册的要求(Requirements in inspection certificates/operating manuals）
4.3 设备标签（Labelling of the device）
4.4 欧盟设计型式试验证书和制造商在防爆方面的符合性声明 （EC design pattern test certificate and manufacturer's declaration of conformity with regard to explosion protection）
5 材料兼容性评估（Material compatibility appraisal）
5.1 传感器（Sensor）
5.2 容器(除传感器、弹性体和"视窗"外) Containment (except sensors, elastomers and "windows")
5.3 光学视窗（Optical windows）
5.4 密封（Seals）
6 检验（Inspections）
6.1 EMC参见IEC 61326-3-1/IEC 61326-3-2，涉及安全功能的故障评估(EMC testing pursuant to IEC 61 326-3-1 , IEC 61 326-3-2, Evaluation of faults with regard to safety function triggering)
6.2 线性误差-根据所选物质的最大偏差和迟滞进行评估。Linearity error – appraisal on the basis of a selected substance with regard to the max. deviation and max. hysteresis.
6.3 T_{90}响应时间（t 90 – step response time）
6.4 信号最大衰减（Signal attenuation at max. load）
图A.1 PCT安全仪表系统(SIS)中分析仪的基础试验程序的说明。

图A.1 安全仪表系统(SIS)中分析仪的基础试验程序



附 录 B

（资料性）

FMEDA －安全评估文件（示例）

图B.1可用于系统地记录过程分析技术(PAT)系统的潜在故障、状态信号和维护间隔等。依据过程分析技术(PAT)系统的设计，可能会引出一些进一步确定PFD的参数。

PAT通道	Q5551

对一个PAT通道的维修时间（故障后的恢复时间,h）	72

维护参数	测试间隔[h]	测试持续时间[h]	诊断覆盖率[%]
安全仪表系统(SIS) 整个检验测试间隔	8760	4	100
PAT系统通道 [例如检测和预测性维护间隔，包括手动调整]	168	0.5	90
PAT系统通道的部分[例如自动分析仪校准间隔]	24	0.05	50

失效序号	对PAT通道的功能安全相关的失效描述和影响[1]	失效分类[D,S]	失效率来源	失效[1/h
1	灯源故障	D	制造商规范	1.2*10
2	采样压力高	D	运行经验	5.8*10
3	冷却故障	D	运行经验	1.2*10
4	采样流量低	D	运行经验	2.3*10
5	采样流量下降	D	运行经验	2.3*10

	自动失效检测			
附加传感器	NO.1	NO.2	NO.3	NO.4
名字	FIA.01 采样	FIA.02 旁路	FIA.03 冷却	分析仪诊断
失效率[h]	$1.2*10^{-4}$	$1.2*10^{-4}$	$5.8*10^{-5}$	$3.8*10^{-5}$
传感器检验测试间隔[h]	24	24	720	168
	NO.1	NO.2	NO.3	NO.4
				×
			×	
		×		
	×			

附 录 C

（资料性）

PFD -数值时间离散测定

对于来自FMEDA的每一个潜在故障，都应指出各自组件的故障率。在此应区分未发现的危险(DU)故障和的已检测到危险(DD)故障。PFD值的确定不包括安全故障。利用这种方法可以检查几个不同的测试间隔。未发现的危险（DU）故障应根据测试间隔进行汇总(例如，在每周检查中检测到的所有故障)，可把持续检测到的危险（DD）故障汇总在一起。

参考文献Kumamoto, H, 1996，相对于长期t，检测到的危险故障与组件i的失效性的关系见公式C.1

$$U_{DDi}(t) = \frac{\lambda_i}{\lambda_i+\mu_i}\left(1 - e^{-(\lambda i+\mu i)t}\right) \approx \frac{\lambda_i}{\lambda_i+\mu_i} \quad \text{.....(C.1)}$$

相对于未检测到的危险故障，组件i的失效性见公式C.2:

$$U_{DUi}(t) = 1 - e^{-\lambda it} \approx \lambda_i t \quad \text{.....(C.2)}$$

发生在不同的时间与组件相关的失效性的确定。

随后在整个测试期间实现平均，该期间应包括最大测试间隔$T_{\max}$。

按测试间隔(PTI)对未发现的危险（DU）故障的失效性进行分组和汇总。

把检测到的危险（DD）故障的失效性汇总在一起，因为他们与测试间隔无关见公式C.3。

$$U_{DD} = \sum_i U_{DD,i} \quad \text{.....(C.3)}$$

通过一个示例，借助电子表格软件程序，说明了整个系统失效性的确定。

示例:有两个不同的测试间隔(PTI1和PTI2，PTI1 = 1周= 168 h, PTI2 = 1年= 8760 h)，可能会发生各种的未发现的危险故障。

此外，还存在其他可知的危险故障。

故障率总和见公式C.4：

$$\lambda_{DU,PT11} = 10^{-7}\frac{1}{h};\ \lambda_{DU,PT12} = 10^{-8}\frac{1}{h};\ \lambda_{DD} = 10^{-7}\frac{1}{h},\mu = 1/5\ 1/h \quad \text{----------(C.4)}$$

时间，h	$U_{DD} = \frac{\lambda_{DD}}{\lambda_{DD}}$			
1	5×10^{-7}	1×10^{-7}	1×10^{-8}	6.1×10^{-7}
2	5×10^{-7}	2×10^{-7}	2×10^{-8}	7.2×10^{-7}
3	5×10^{-7}	3×10^{-7}	3×10^{-8}	8.3×10^{-7}
…				
168	5×10^{-7}	0	1.68×10^{-6}	1
169	5×10^{-7}	1×10^{-7}	1.69×10^{-6}	2.29×10^{-6}
170	5×10^{-7}	2×10^{-7}	1.70×10^{-6}	2.40×10^{-6}
…				
8759	5×10^{-7}	$2,3\times10^{-6}$	8.759×10^{-5}	9.039×10^{-5}
8760	5×10^{-7}	$2,4\times10^{-6}$	0	1

如果在测试期间不能检测到全部故障(PTC < 100%)，则应在测试后检查与时间相关的失效性后，将失效性的偏移量添加进去。

对于多通道系统，应相对于通道配置来确定整个系统的失效性。

在这方面，参考文献Gabriel, T.，2010:

$$U_{1001}(t) = U_{ch1}(t)$$

$$U_{1002}(t) = U_{ch1}(t)\cdot U_{ch2}(t)$$

$$U_{1003}(t) = U_{ch1}(t)\cdot U_{ch2}(t)\cdot U_{ch3}(t)$$

$$U_{2003}(t) = (U_{ch1}(t)\cdot U_{ch2}(t))+(U_{ch2}(t)\cdot U_{ch3}(t))+(U_{ch1}(t)\cdot U_{ch3}(t))-2(U_{ch1}(t)\cdot U_{ch2}(t)\cdot U_{ch3}(t))$$

不考虑常见故障引起的整个系统故障概率值见公式 c.5。

$$PFD_{MOON} = \frac{1}{T_{max}}\sum U_{MOON}(t) \quad \text{……} \quad \text{(C.5)}$$

当系统由多个通道组成时,按需故障概率值（*PFD*）应包括共同原因引起的故障，然而，这种故障一般由单独通道引发，该故障用ß表示，见公式C.6。

$$PFD_{beta} = \beta \times \frac{1}{T_{max}}\int_0^{T_{max}} U_{1001}(t) \quad \text{……..} \quad \text{(C.6)}$$

整个系统的按需故障概率值见公式C.7。

$$PFD_{PAT}=PFD_{MOON}+PFD_{beta} \quad \text{……..} \quad \text{(C.7)}$$

按上述步骤可准确测定按需故障概率值（*PFD*），通常，可借助电子表格软件程序来计算。

参考文献

【1】 IEC TR 61813:2011 On-line analyser systems – Guide to design and installation
【2】 IEC TR 61832:2015 Design and installation of on-line analyser systems – Guide to technical enquiry and bid evaluation
【3】 IEC TR 62010:2016 Analyser system – Maintenance management
【4】 IEC 61285:2015 Industrial-process control – Safety of analyser houses
【5】 Kumamoto,H.,Heniey, E.,1996: Probabilistic Risk Assessment ang Management for Engineers and Scientists, IEEE Press
【6】 Gabriel, T., 2010: Generic Construction of Availability Calculation Model for Safety Loops in Process Industry, Dissertation Technische Universitat Kaiserslautern (University of Kaiserslautern