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 44564—2024/IEC TR 63176:2019

安全仪表系统　过程分析技术系统

Safety instrumented systems—Process analysis technology systems

（IEC TR 63176:2019，Process analysis technology systemes as part of safty instrumented systems，IDT）

2024-09-29 发布　　2025-04-01 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 TR 63176:2019《过程分析技术系统作为安全仪表系统的一部分》。文件类型由IEC技术报告调整为我国的国家标准化指导性技术文件。

本文件做了下列最小限度的编辑性改动：

——为与现有标准协调，将标准名称改为《安全仪表系统　过程分析技术系统》；

——补充了3.2U_{MooN}中MooN的解释内容；

——为附录C中公式编排序号。

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：中国仪器仪表行业协会、机械工业仪器仪表综合技术经济研究所、福建顺昌虹润精密仪器有限公司、北京北分瑞利分析仪器(集团)有限责任公司、北京雪迪龙科技股份有限公司、西克麦哈克(北京)仪器有限公司、吉林大学、北京北分麦哈克分析仪器有限公司、聚光科技(杭州)股份有限公司、山东鲁南瑞虹化工仪器有限公司、浙江福立分析仪器股份有限公司、江苏方天电力技术有限公司、重庆川仪分析仪器有限公司。

本文件主要起草人：闫海荣、熊文泽、林善平、陈景卫、郜武、李长云、高德江、陈淼、俞大海、蒋鸿照、李俊珂、叶加星、熊彬烽、黄亚龙、荣继武。

引　言

本文件用于帮助使用过程分析仪的用户，按照安全仪表系统(SIS)要求安装使用设备。本文件中可能涉及安全相关的约束性条款的内容，但整体文件内容是推荐性的。例如，过程分析技术(PAT)测量设备，在过程工业中被用作SIS的传感器组件，在大多数情况下，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，能够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，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系统性失效，通过短时间内定期检查测量设备能够避免此问题的发生。

由于过程分析测量变量和方法的多样性，且在每种情况下受信号、准确度的限制，应用的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(所有部分)进行功能安全性的定量评估。除作为SIS组件性能评估欠缺外，相似的应用数量也太少。然而，在过去的三十年里，过程分析仪企业已成功将数百个PAT测量设备应用到SIS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能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(所有部分)中有描述，在IEC 61511(所有部分)中规定了SIS。本文件描述了PAT测量设备作为SIS一部分的程序指引。

安全仪表系统　过程分析技术系统

1　范围

本文件给出了安全设备认证的所有必要步骤，并通过扩充对 PAT 测量设备的特殊要求来补充 SIS 设备的安全管理。

本文件适用于过程工业 SIS 中 PAT 测量设备的规划、安装和运行(维护)。

本文件不涉及整个 SIS 设备的安全管理。

本文件使用的术语“鉴定”专指 PAT 系统用于 SIS 设备的适用性测试，与制药环境中使用的术语“鉴定”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。

GB/T 20438.6—2017　电气/电子/可编程电子安全相关系统的功能安全　第 6 部分：GB/T 20438.2和 GB/T 20438.3 的应用指南(IEC 61508-6:2010，IDT)

GB/T 21109.1—2022　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、硬件和应用编程要求(IEC 61151-1:2016，IDT)

IEC 61508(所有部分)　电气/电子/可编程电子安全相关系统的功能安全(Functional safety of electrical/electronic/programmable electronic safety-related systems)

注：GB/T 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

IEC 61511(所有部分)　功能安全　过程工业领域用安全仪表系统(Functional safety—Safety instrumented systems for the process industry sector)

注：GB/T 21109(所有部分)　过程工业领域安全仪表系统的功能安全[IEC 61511(所有部分)]

3　术语、定义、符号和缩略语

3.1　术语和定义

下列术语和定义适应于本文件。

ISO 和 IEC 维护的用于标准化的术语数据库网址如下：

——IEC 电工百科：https://www.electropedia.org/

——ISO 在线浏览平台：https://www.iso.org/obp

3.1.1

PAT 测量设备　process analysis technology(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，还有仪表柜、分析小屋或站房。

3.1.2

基础测试 basic testing

为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，包括使用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进行类似测量任务而获得的实际使用经验。

3.1.5

运行中测试 in-service testing

在生产运行期间，监控SIS中的PAT系统的运行。

注1：在此可明确验证PAT系统的操作性能程序与相应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

性能证明 proven performance

过程分析仪安装是否适合作为SIS的一部分做出最终判定的全部证明。

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证明。

注2：由专家团队最终确定PAT系统性能证明，其确定方式与通常用于现场设备和逻辑解算器（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值和输出值之间的关系，输入值为被测物理量，输出值为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参考值，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

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：有下列几种情况：

——有内置在PAT系统的诊断传感器（如流量计）；

——有内置在PAT系统的通道（如自动校准）；

——有内置在PAT系统的通道（如自检、手动调校和维护）；

——整个系统（包括手动、PAT和SIS的其他部分）。

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

检验测试覆盖率　proof test coverage

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，该通道未能诊断到的危险(DU)故障率会因为丧失功能而增加，而能诊断到的危险(DD)故障率会降低。自动校准通常仅在足够短的时间间隔内检查一定的 DU 故障率，也不排除出现在经过核查和维护后仍未发现该通道故障的情况。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。

3.2　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：能诊断到的危险(dangerous detected)

DU：未能诊断到的危险(dangerous undetected)

FAT：工厂验收测试(factory acceptance test)

FMEA：失效模式和影响分析(failure mode and effects analysis)

FMEDA：失效模式、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(process analysis 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)

PTC：检验测试覆盖率(proof test coverage)

S：安全(safety)

SAT：现场验收测试(site acceptance test)

SFF：安全失效分数(safe failure fraction)

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 instrumented system)

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 组件由于 DD 失效导致的不可用

$U_{DU,i}$：第 i 组件由于 DU 失效导致的不可用

U_{ch1}：通道 1 不可用性

U_{MooN}：整个系统在 MooN 配置的不可用性，MooN：N 中取 M 表决结构

β：共因失效的比例

T_{max}：最大测试间隔

PFD_{beta}：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 PAT 系统的 PFD 值

4 审核程序

4.1 概述

PAT 测量设备通常是复杂 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 有足够丰富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（见图 1）。包括 PAT 系统的安装工程人员和岗位操作人员（见 4.2 和 4.3），并记录每个审核步骤。

认证过程由 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参与。所有与 PAT 系统性能相关的过程数据由负责安全的工程师确认。

当几种测量方法都技术可行时，宜对这些方法进行考查和评估。从计划一开始宜考虑进一步减少/最小化 PAT 系统整体失效概率的问题，包括：

——冗余程度/故障裕度；

——同质或多样性冗余；

——其他测量设备的操作经验/性能证明；

——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，宜考虑监测测量值的偏差。

测量方法选择后，确定样品处理过程方案和相关部件的设计，部件的设计和选型都要进行功能性论证并归档。宜使用合适的和可靠的设备与部件来搭建 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。

当假设安装工程人员和/或工厂操作人员就特定应用上的经验（比如失效率、检验测试间隔等）高于制造商时，可在不考虑制造商的建议情况下，负责对特定应用开展安全完整性等级（SIL）分级。虽然宜优先使用经过 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，也可考虑使用未经 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用于单通道 SIL2 的应用。

对于 PAT 测量设备，宜对整个 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。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 SIS 的整体 PFD 值估算中加以考虑。

性能证明时，合格的硬件故障裕度（HFT）值（见 4.5.5）和 PFD 值（见 4.5.7）在可用的情况下，PAT 系统对 SIS 的适用性宜作为最终衡量标准进行考虑。

由于过程分析设备的复杂性，安全失效分数（SFF）是不充分的。因此，没有对 SFF 开展评估，也没有将 SFF 评估作为 PAT 系统的指标。

如果没有足够的数据来支持性能证明，但是测量方法已经成功用于类似的应用中，PAT 系统作为 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。

作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，PAT 测量设备的生命周期宜从试运行到停运全程记录存档。

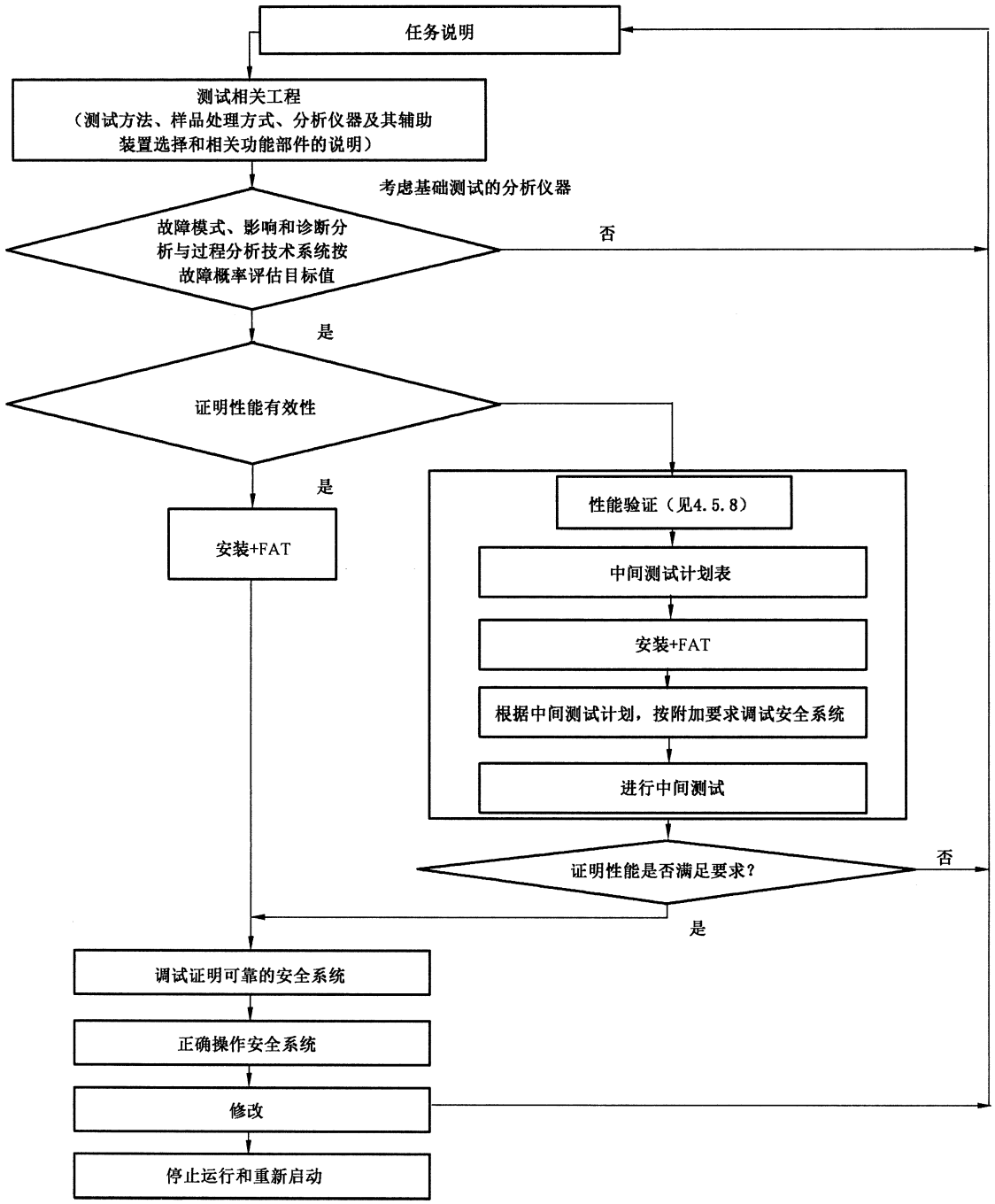

图 1　PAT 测量系统认证过程层级

4.2　安装工程人员要求的建议

下列要求来自于 GB/T 21109.1—2022 中 5.2，详细阐述了 PAT 处理措施。作为 SIS 一部分的 PAT 装置的安装核查需要对 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，可由专家团队将这些知识和经验总结用于指导鉴定工作。参与实施生命周期安全的人员、部门或组织宜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。

专家团队宜具备下列知识和经验。

——了解测量现场的化学或物理流程。

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流程中的可用性(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。如果没有在安全功能中明确排除,则启动和停运宜与正常生产操作一样加以考虑。

——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。

有能力进行失效模式、影响和诊断分析(FMEDA),评估PAT系统的PFD,并有能力配合进行风险分析[比如:危害性和可操作性研究(HazOp),用于预知,事故原因审核,效能评估和对策]是必要的。

——应用的法规和标准的知识。

本文件涉及设计的相关法规和标准按IEC 61508(所有部分)和IEC 61511(所有部分)执行。

4.3 岗位操作人员要求的建议

下列要求来自GB/T 21109.1—2022中6.2,并就PAT相关内容进行了具体规定。按照SIS安装的PAT测量设备的操作人员宜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等级。如果SIS需保持功能安全性方式运行和维护,建议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(所有部分)规定的要求外,还宜具备下面的知识、技能和经验。

——PAT系统功能性的知识。

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。

——PAT设备维护的技能和经验。

熟悉PAT测量系统的机械和电气工作,包括维修和维护工作,有识别失效的经验(例如,测量系统的偶发故障,不能正常工作)。

4.4 基础测试(仅限分析仪)

安全系统中使用的每一台分析仪都宜满足基本质量要求。基础测试有助于检验这些质量要求(见附录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性能证明。

由于基础测试的结果由分析仪的硬件和软件所决定,要确保制造商主动并及时向最终用户报告硬件或软件的更改。此后,工厂操作员宜根据具体情况决定是否更新基础测试。如果制造商开发的分析仪符合IEC 61508(所有部分)的质量要求,基础测试一般不需要更新。

4.5 工程设计

4.5.1 总则

因为对SIS后续运行的有效性有决定性影响,作为SIS一部分的PAT测量设备的安装设计宜严谨。

从根本上说,PAT系统的工程设计基于包括所有物理和化学性质(压力、温度、成分、相态、露点等)

的工艺技术参数表。

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抽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,可能出现这样的情况: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 SIS 不可分割的一部分,宜在 PFD 测定过程中予以考虑。

在某些情况下,样品处理会严重影响 PAT 系统传感器安装的 PFD 值。为此,PAT 系统配备了附加的传感器,可在尽可能短的时间内识别样品处理错误,降低现存的 DU 故障,转变为 DD 故障。

除了验证测试之外,与传统的安全系统相比,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 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

作为 SIS 一部分的 PAT 测量装置的设计基于以下原则。

——SIF 的定义。

功能安全的性能水平(如 SIL),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 PAT 中,这通常涉及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 PAT 设计时宜虑到这一点,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。

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,宜考虑特殊系统条件(如启动、关闭、负载变化、故障)的影响。

4.5.3 含应用的分析仪

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

具体的计量适用性可通过现有的可比性的应用确定,但是,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宜记录下来。

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。

样品处理宜包含诊断功能,以便能识别出影响安全功能的故障并发出信号(避免 DU 失效或 DU 转化为 DD)。

在可能的情况下,外围设备宜包含已验证运行可靠的组件。

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

4.5.5 HFT

HFT 提供关于系统冗余程度的信息,见 GB/T 21109.1—2022 中 11.4,表 1 中列出了硬件故障裕度。

表 1 SIL 中最小硬件故障裕度要求

SIL	运行中测试最小硬件故障裕度	经充分性能证明后最小硬件故障裕度
1	0	0
2	1	0
3	2	1

性能证明对于 SIS 中的 PAT 系统是必要的(见第 4 章),这对应到基于早期应用的选择(GB/T 21109.1—2022 中 11.5)。

在性能得到充分证明的情况下,只有在 PAT 系统中仅能配置与过程相关的参数并保护此设置时,才能用最小硬件故障裕度。性能证明期间编写的 PAT 系统或分析仪软件宜进行解释说明和记录,并重新开始检验测试。

4.5.6 PAT 系统的 FMEDA

宜对整个 PAT 系统进行失效概率和影响分析,包括供电、比对和辅助介质(如 FMEDA)。对在此期间观察到的失效进行描述并适当分类(如 DD 、DU、S),列出失效率(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)。潜在失效由专家团队识别,并确定其失效率。识别出的故障宜进一步按随机性和系统性进行分类。尽可能对系统性故障进行补救,如果不行,系统故障宜通过诊断设备来识别。PAT 系统的定期检验测试宜做到覆盖率达到 100%。如果估计检验测试覆盖率偏低,该保守的评估值宜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,宜遵守所有相关的正确操作条件。

FMEDA 的范围取决于 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)。同理,在故障模式下,通过其他合适的方式(如不断变换切换点),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 PFD_{PAT}的估算

PFD_{PAT}值用于统计 PAT 测量系统要求的失效概率,此值代表安全系统要求的失效概率的一部分。在所有情况下,在整体估算中宜考虑进一步要求的 PFD(如:逻辑或驱动器相关)。在某些情况下,可通过附加状态信号 DU 失效转化为 DD 失效和/或减少维护间隔来降低 PFD_{PAT}值。否则,测量系统宜在必要时改变或增加通道的数量。PFD_{PAT}值过高最终判别排除作为 SIS 的测量装置。

PFD_{PAT}值宜采用相应的过程确定。下面以示例的方式说明数值离散方法。

基于系统分部件随时间 t 的失效性,是利用电子表格分析,来实现确定要求的 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不可用性 $U(t)$来确定的。

首先通过 FMEDA 记录潜在故障,并将其分为 S、DD 和 DU,这些故障是形成失效性的基本条件。

普遍使用平均不可用性 $U(t)$的公式,并构成 GB/T 20438.6—2017 中用于计算 PFD 值的公式的基础。

具体方法见附录 C。

4.5.8 性能证明——对 PAT 系统进行各种不同的运行中测试

利用充分的操作经验,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,可通过

运行中测试来获得性能证明。

完成材料流程图、零件清单和 PFD_{PAT} 值估算后，确定是否有可比性的 PAT 测量系统的足够的操作经验。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 PAT 测量系统进行运行中测试，在所有操作条件下，在设定的测量位置进行。运行中测试在下述条件下进行：

——可预计完成后的运行中测试有好的结果；

——估算 PFD_{PAT} 值足够低(如：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，则不宜通过运行中测试来获得性能证明；

——部分规划好的 PAT 部件宜已经成功地使用在类似的位置；

——在运行中测试阶段，安全功能宜根据具体情况补充附加测量；

——在开始安装之前，宜记录运行中测试和评估标准，以便用于以后性能证明的测定；

——如果最终性能证明无法验证，则宜在必要时以另一种方式并通过 PAT 以外的方法来保证安全功能。这意味着 PAT 方法不适用这种情况。

借助于运行中测试，可确立新的分析仪或新的样品处理的安全功能。

4.5.9 PAT 系统的安全逻辑

作为 SIS 装置的一部分，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的单元。

原则上，逻辑器件可在主控制系统或上级安全相关的控制器(PLC)或逻辑解算器中实现，置于单独 PAT 控制器(PLC、安全相关的 PLC 或逻辑解算器)中，或完全集成在分析仪中，也可是混合形式。

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，在所有情况下都视其为误差来源。由于切换阀故障导致的 DU 失效，可通过位置指示器转换为 DD 失效。此外，可考虑将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宜在 PFD 值预估的背景下确定。理想情况下，这些定期测试能识别所有潜在的 DU 和空闲监测装置，包括位置指示器、液位、流量、压力或温度限值传感器。

估计周期性测试检测到所描述的故障的概率。在估算 PFD 值时，考虑这个检验测试的覆盖范围。

测试间隔对 PFD 值有相当大的影响。

4.6 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。如果没有经过性能证明，调试可与运行中测试同时进行。运行和维护人员宜进行培训。

4.7 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的安全评价危害性摘要；

——工艺过程数据分析工作表；

——分析仪、技术参数表；

——物料流程图及零件清单 PAT 流程图(P&I),PAT 工艺流程图(P&ID);
——分析仪/部件文件(如 SIL 证书);
——估算 PFD,包括 FMEDA 协议;
——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;
——专家姓名;
——分阶段进行运行中测试的计划表和记录。

5 常规运行

5.1 总则

第 5 章提到的所有任务都宜由安全系统的操作人员实施。

5.2 运行期间的周期性测试

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

检验宜记录在检测报告中。宜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—执行器宜与相关的其他任务进行协调和执行,见GB/T 21109.1—2022 中 5.2.1~5.2.3。

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 PAT 系统。

5.3 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定期进行测试(见 5.2),并保存记录,见IEC 61511(所有部分)。

这些记录至少包含以下信息。

5.3.2 维护计划表

维护和检验计划表(M+I 计划表)描述了在各个时间间隔内执行的工作。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。

不超过定义的 MTTR 持续时间,因为 4.5.7 中确定的 PFD 值直接取决于这些持续时间。

5.3.3 作业指导书

根据测试规范(见 4.7)进行的检验在作业指导书中给出说明。

5.3.4 工作记录

在5.2中提及的检测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

整个系统每次运行维护都宜做记录，包括样品处理在内。

每次装置故障可按5.3.4给出的需要记录文件的内容分类：

——故障位置(过程分析仪、样品处理)；

——故障检测(如检验测试)；

——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 故障数据的评价和偏差处理

在持续改进过程的背景下，生产设备操作人员和PAT专家宜对故障数据进行评价，以缩小相对于正确运行的偏差。

5.5 修改

5.5.1 PAT系统的修改

在修改安全系统配置时，比如在某种情况下会存在不经意或错误的执行，而导致系统性故障风险，进而削弱安全系统预期实现的动作。在这种情况下，PFD值改变了，这意味着可能不再符合所需的SIL分类标准。在对修改进行评估时，采用与规划和安装现有安全系统时相同的系统。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，视为修改，并将被检查。此情况适用于硬件和软件。如制造商对安全系统部件进行软件和硬件的修改，则制造商宜给出报告。

如果软件开发依据IEC 61508(所有部分)，则可免除软件的更新测试。

5.5.2 过程工艺的修改

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，评估和记录其对安全适用性的影响。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，仅从流程中断开不代表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，运行中测试阶段可省略(见 5.5.2)。

5.7 溯源性

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

附 录 A
（资料性）
分析仪基础试验项目

基础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。

基础试验项目内容如下。

A.1 组织检查

A.1.1 类型/版本
A.1.2 测量范围、传感器
A.1.3 系列号
A.1.4 硬件
A.1.5 软件
A.1.6 文档
A.1.6.1 文档版本号
A.1.6.2 理解程度
A.1.6.3 正确性
A.1.6.4 完整性
A.1.6.5 操作和安全说明

A.2 分析仪制造商规范

A.2.1 开发参见 IEC 61508(所有部分)的 SIL2 或 SIL3
A.2.2 EMC 参见 IEC 61326-3-1:2017/IEC 61326-3-2:2017
A.2.3 未能诊断到的危险失效率
A.2.4 能诊断到的危险失效率
A.2.5 未能诊断到的安全失效率
A.2.6 能诊断到的安全失效率
A.2.7 测量功能的设计型式试验证书
A.2.8 允许的湿度
A.2.9 环境温度范围
A.2.10 环境温度影响
A.2.11 过程温度范围
A.2.12 过程温度影响
A.2.13 过程压力范围
A.2.14 过程压力影响
A.2.15 振动影响

A.3 维护评估

A.3.1 设计
A.3.2 职业安全
A.3.3 操作性

A.3.4 重新设置为默认设置的能力
A.3.5 锁定参数
A.3.6 故障信号
A.3.7 服务请求信号
A.3.8 服务信号
A.3.9 维护费用
A.3.10 维护友好性
A.3.11 接受对制造商设备的经验数据的评估

A.4 防爆评估

A.4.1 与其他装置互联的能力
A.4.2 检验证书/操作手册的要求
A.4.3 设备标志
A.4.4 设计型式试验证书和制造商在防爆方面的符合性声明

A.5 材料兼容性评估

A.5.1 传感器
A.5.2 容器(除传感器、弹性体和"视窗"外)
A.5.3 光学视窗
A.5.4 密封

A.6 检验

A.6.1 EMC 参见 IEC 61326-3-1:2017/IEC 61326-3-2:2017,涉及安全功能的故障评估
A.6.2 线性误差:根据所选物质的最大偏差和迟滞进行评估
A.6.3 T_{90}响应时间
A.6.4 信号最大衰减

图 A.1 给出 PCT 在 SIS 中分析仪的基础试验程序的说明示例。

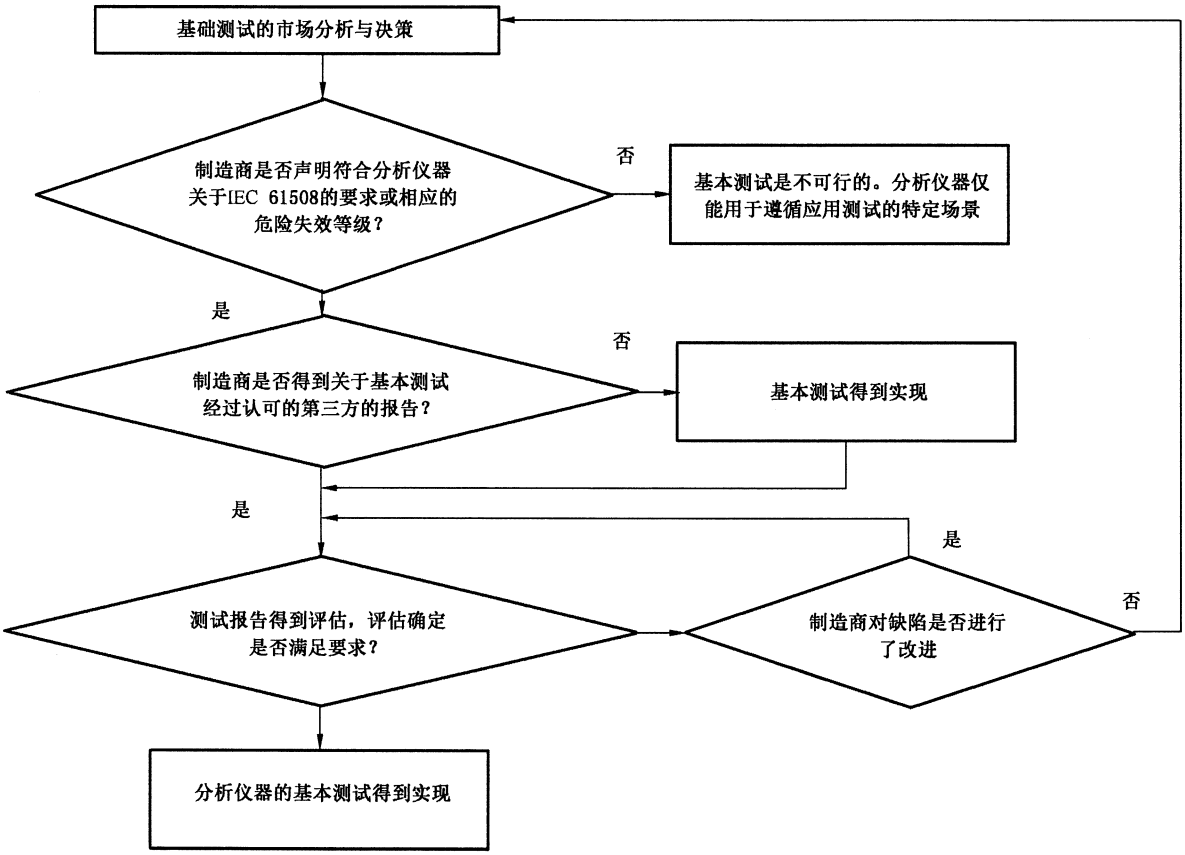

图 A.1　SIS 中分析仪的基础试验程序

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 PAT 系统的潜在故障、状态信号和维护间隔等。依据 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

常见原因	0.05

维护参数	测试间隔 h	测试持续时间 h	诊断覆盖率 %
SIS 整个检验测试间隔	8 760	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	失效率 h^{-1}
1	灯源故障	D	制造商规范	1.2×10^{-7}
2	采样压力高	D	运行经验	5.8×10^{-4}
3	冷却故障	D	运行经验	1.2×10^{-4}
4	采样流量低	D	运行经验	2.3×10^{-6}
5	采样流量下降	D	运行经验	2.3×10^{-7}

	自动失效检测			
附加传感器	1	2	3	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}	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
	1	2	3	4
				×
			×	
		×		
	×			

图 B.1 可用于系统地记录 PAT 系统的潜在故障、状态信号和维护间隔

附 录 C
（资料性）
PFD 值时间离散测定

对于来自 FMEDA 的每一个潜在失效，宜指出各自组件的失效率。在此区分 DU 和 DD。PFD 值的确定不包括安全失效。利用这种方法可检查几个不同的测试间隔。DU 失效根据测试间隔进行汇总（例如在每周检查中检测到的所有失效），可把持续 DD 汇总在一起。

参考文献 Kumamoto，H，1996，相对于长期 t，DD 与组件 i 的失效性的关系见公式(C.1)：

$$U_{DD,i}(t)=\frac{\lambda_i}{\lambda_i+\mu_i}[1-e^{-(\lambda_i+\mu_i)t}]\approx\frac{\lambda_i}{\lambda_i+\mu_i} \quad \cdots\cdots(C.1)$$

相对于 DU 失效，组件 i 的失效性见公式(C.2)：

$$U_{DU,i}(t)=1-e^{-\lambda_i t}\approx\lambda_i t \quad \cdots\cdots(C.2)$$

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，该期间包括最大测试间隔 T_{max}。

按测试间隔(PTI)对 DU 失效的失效性进行分组和汇总。

把 DD 失效的失效性汇总在一起，因为它们与测试间隔无关，见公式(C.3)。

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

下面通过一个示例借助电子表格软件程序说明整个系统失效性的确定。

示例中假设有两个不同的测试间隔(PTI1 和 PTI2，PTI1 = 1 周= 168 h，PTI2＝1 年＝8 760 h)，可能会发生各种 DU。

此外，还存在其他可知的危险失效。

失效率总和见公式(C.4)，计算结果列入表 C.1。

$$\lambda_{DU,PTI1}=10^{-7}h^{-1};\lambda_{DU,PTI2}=10^{-8}h^{-1};\lambda_{DD}=10^{-7}h^{-1},\mu=1/5\ h^{-1} \quad \cdots\cdots(C.4)$$

表 C.1 不同测试间隔情况下安全参数计算示例

时间/h	$U_{DD}=\frac{\lambda_{DD}}{\lambda_{DD}+\mu}$	$U_{DU,PTI1}(t)=\lambda_{DU,PTI1}t$	$U_{DU,PTI2}(t)=\lambda_{DU,PTI2}t$	$U_{ch1}(t)=U_{DU,PTI1}(t)+U_{DU,PTI2}(t)+U_{DD}$
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}
…				
8 759	5×10^{-7}	$2,3\times10^{-6}$	8.759×10^{-5}	9.039×10^{-5}
8 760	5×10^{-7}	$2,4\times10^{-6}$	0	1

如果在测试期间不能检测到全部失效(PTC ＜ 100%)，则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：

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

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

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

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

不考虑常见失效引起的整个系统失效概率值见公式(C.5)。

$$PFD_{MooN}=\frac{1}{T_{max}}\Sigma U_{MooN}(t) \qquad \cdots\cdots(C.5)$$

当系统由多个通道组成时，PFD 值应包括共同原因引起的失效，然而，这种失效一般由单独通道引发，该失效用 β 表示，见公式(C.6)。

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

整个系统的 PFD 值见公式(C.7)。

$$PFD_{PAT}=PFD_{MooN}+PFD_{beta} \qquad \cdots\cdots(C.7)$$

按上述步骤可准确测定 PFD 值，通常，可借助电子表格软件程序来计算。

参 考 文 献

[1] IEC 61285:2015 Industrial-process control—Safety of analyser houses

[2] IEC 61326-3-1:2017 Electrical equipment for measurement, control and laboratory use—EMC requirements—Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—General industrial applications

[3] IEC 61326-3-2:2017 Electrical equipment for measurement, control and laboratory use—EMC requirements—Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—Industrial applications with specified electromagnetic environment

[4] IEC TR 61831:2011 On-line analyser systems—Guide to design and installation

[5] IEC TR 61832:2015 Design and installation of on-line analyser systems—Guide to technical enquiry and bid evaluation

[6] IEC TR 62010:2016 Analyser system—Maintenance management

[7] Kumamoto,H.,Heniey, E.,1996: Probabilistic Risk Assessment ang Management for Engineers and Scientists, IEEE Press

[8] Gabriel, T., 2010: Generic Construction of Availability Calculation Model for Safety Loops in Process Industry, Dissertation TechnischeUniversitat Kaiserslautern (University of Kaiserslautern

中 华 人 民 共 和 国
国家标准化指导性技术文件
安全仪表系统　过程分析技术系统
GB/Z 44564—2024/IEC TR 63176:2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.75　字数 38 千字
2024年9月第一版　2024年9月第一次印刷
*
书号:155066·1-77379　定价　49.00 元

GB/Z 44564-2024