T/CECS ×××—202X

中国工程建设标准化协会标准

油气管道智能传感器安全完整性评测标准

Safety integrity test and assessment standard for intelligent sensor in oil and gas pipeline

×××出版社

中国工程建设标准化协会标准

油气管道智能传感器安全完整性评测标准

Safety integrity test and assessment standard for intelligent sensor in oil and gas pipeline

T/CECS　XXX-202X

主编单位：机械工业仪器仪表综合技术经济研究所

批准单位：

施行日期：

前　　言

根据中国工程建设标准化协会《关于印发<2023年第二批协会标准制定、修订计划>的通知》（建标协字[2023]50号）的要求，编制组经深入调查研究，认真总结实践经验，参考国内外先进标准，并在广泛征求意见的基础上，制定本标准。

本标准共分5章，主要内容包括：总则、术语、基本规定、评测管理、评测内容、评估报告等。

本标准的某些内容可能直接或间接涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准由中国工程建设标准化协会功能安全与信息安全专业委员会归口管理，由机械工业仪器仪表综合技术经济研究所负责具体技术内容的解释。执行过程中，如有意见或建议，请反馈给机械工业仪器仪表综合技术经济研究所（地址：北京市西城区广安门外大街甲397号，邮编100055，邮箱：fscn@instrnet.com）。

主编单位：

主要起草人：

主要审查人：

目　次

Contents

1 总 则

1.0.1 为规范油气管道智能传感器的安全运行要求，保证油气管道高效可靠的安全数据感知能力，制定本标准。

1.0.2 本标准适用于油气管道智能传感器选型、验收时的安全完整性评测。

1.0.3 本标准所定义的传感器包括执行油气管道生产运行过程中的安全传感组件，在具体的应用中可能称为开关、变送器、探测器等。

1.0.4 油气管道智能传感器安全完整性评测除应符合本标准的规定外，尚应符合国家现行有关标准和现行中国工程建设标准化协会有关标准的规定。

2 术 语

2.0.1 安全完整性等级 safety integrity level SIL

一种离散的等级（四个可能等级之一），对应安全完整性量值的范围。安全完整性等级 4 是最高的，安全完整性等级 1 是最低的。

2.0.2 系统性能力 systematic capability

当一个组件按组件符合项安全手册的规定应用时，针对规定的组件安全功能，组件的系统性安全完整性满足规定的 SIL 要求的置信度的度量（表示为 SC1 到 SC4）。

2.0.3 运行模式 mode of operation

安全相关系统运行的方式，可为下列之一：

1 低要求模式：仅当要求时才执行将 EUC 导入规定安全状态的安全功能，并且要求的频率不大于每年一次；

2 高要求模式：将 EUC 导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率大于每年一次；

3 连续模式：安全功能将 EUC 保持在安全状态是正常运行的一部分。

2.0.4 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。

2.0.5 系统性失效 systematic failure

原因确定的失效，只有对设计或制造过程、操作规程、文档或其他相关因素进行修改后，才有可能消除这种失效。

2.0.6 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：

1 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。

2 降低在要求时安全功能正确执行的概率。

2.0.7 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：

1 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

2　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。

3 基 本 规 定

3.0.1 本标准规定在油气管道应用中，当智能传感器用于安全防护功能时，应对其选型、验收过程中开展安全完整性等级（SIL）评测的要求。

3.0.2 本标准限定的评测等级为 SIL1、SIL2 和 SIL3。

3.0.3 本标准是对于安全回路中传感单元的安全能力评测要求，对于整个安全回路的评测或评估要求不在本标准范围之内。

3.0.3 本标准所规定的评测活动应由具备国家或国际认可资质的认证机构执行，并出具相应的评测报告。

4 评 测 管 理

4.0.1 应建立一套系统化的管理程序来对于油气管道智能传感器的评测过程进行规划、实施和归档。

4.0.2 实施评测的组织或人员应与传感器的研制或供应方具有独立性。

4.0.3 应将评测相关的活动和收集的证据形成文档，在评测完成后应形成正式的针对特定项目的传感器安全完整性评测报告。

4.0.4 应对实施评测的人员进行明确分工，应至少规定评测负责人。

5 评 测 内 容

5.1 评测计划的编制

5.1.1 应在评测开始前编制评测计划。

5.1.2 评测计划应至少包括如下内容：

1 应规定评测对象的范围，一个评测计划可包含多个传感器，包括传感器本身的物理边界，传感器可应用的安全功能及其安全完整性情况等；

2 应定义评测时间安排；

3 应规定评测人员安排，包括对于评测人员的能力要求，如人员所具备的功能安全知识，以及对于智能传感器的了解程度等；

4 应对人员的独立性进行专项评价，确保参与评测的人员与智能传感器的研制和供应单位无关联关系；

5 应规定可能使用的评测工具，包括对于工具的置信度的要求；

6 应规定评测应达到的目标，包括应遵循的标准规范和油气管道的应用要求。

5.2 评测目标的构建

5.2.1 评测目标应至少包括如下内容：

1 传感器预期应用安全仪表功能（SIF）的 SIL 能力及相关的功能安全参数；

2 传感器满足应用要求应达到的最长响应时间、故障响应时间等；

3 传感器所应用的环境条件要求，包括温度、湿度、电磁环境等；

4 传感器所适用的测量介质的要求；

5 传感器应达到的安全测量精度；

6 传感器满足特定 SIL 应用情况下的检验测试要求，包括检验测试间隔和检验测试覆盖率；

7 传感器在油气管道现场应用的其他安装、使用和操作维护的限制。

5.2.2 评测目标的获得可来自于如下文件或资料：

1 传感器所应用项目的整体安全要求规范（SRS）、现场实际工艺或环境状

态；

2　该类传感器与功能安全和油气管道相关的标准或行业惯例；

3　传感器制造商所提供的安全手册和用户手册。

5.2.3　评测目标应形成正式的文件，在整个评测过程中保持可追溯性，并被评测活动所全部覆盖。

5.3　评测的实施

Ⅰ　基本要求

5.3.1　可以通过以下两种方式之一来评测传感器在应用项目中可能能够实现的安全完整性等级：

1　方式一：传感器的研制已经通过了第三方 SIL 评测认证，检查该评测认证的相关资料，确认其规范有效，且满足当前油气管道的应用限制；

2　方式二：传感器在油气管道或相近环境条件下有较多数量或较长时间的现场应用，按照 GB/T 21109.1 中“以往使用”的要求满足相应的安全完整性能力。

5.3.2　对于方式一应检查第三方 SIL 认证机构是否具备国家或国际认可的资质，确认制造商能够提供有效的评测认证证书、报告、安全手册等材料。

5.3.3　应检查制造商提供的安全手册和用户手册，以确保其描述的安全使用限制符合特定油气管道现场的应用要求。

5.3.4　对于方式二应按照 GB/T 21109.1—2022 的 11.5 的要求执行评测。

5.3.5　为执行方式二的评测，应获得待评测传感器在相似环境下的有效运行经验，具体包括：

1　传感器的运行经历和失效统计过程应在一套适当的管理体系下执行，运行经验证据应可审查；

2　运行经验证据应与传感器软件和硬件的精确已知版本、配置设置相关联，如果认为运行经验具有通用性能够适用于传感器的各个版本，则应分析不同版本之间的差异并证明这种通用性；

3　传感器在类似环境条件下的使用统计累计时长，以及具体的环境特征条件（如温湿度等）；

4　应有一套可靠性失效报告体系，来对运行过程中发生失效的详细记录，包

括发现失效的时间、现场失效的具体表现（例如失电、机械磨损等）、失效的原因机理分析（如存在）、采取的补救或更换手段等；如果对失效报告体系存在不确定的情况，应对预估的运行时间统计进行减少，例如减少传感器运行时间 30%；应确保是失效的记录是现场传感器发生失效之后的原始情况，而不是基于操作员或技术人员的主观判断；

5　对运行经验证据的分析应考虑待评测传感器的特定功能是连续运行还是间歇按需运行。在第一种情况下，证据的依据应是实际运行的小时数；在后者中，证据的依据应是在按需功能没有失效情况下的执行次数；

6　运行经验的时长应根据所需满足的 SIL 目标确定、传感器的复杂性等因素来确定，SIL 等级越高、传感器越复杂所需最低运行时长越长；

7　通过运行经验结合统计学相关的分析，可以计算获得传感器基于运行经验的随机失效率，如果该数值远大于理论分析数值，则应分析是传感器内存在明显的系统性失效还是固有的随机失效过大；

II 功能和性能的适应性评测

5.3.6　应对智能传感器的安全相关和非安全相关功能及其安全相关性能开展适应性评测，以证明：

1　传感器是否按照预期的油气管道应用场景执行了所需的功能；

2　是否仅执行了这些所需的功能，额外的非安全相关功能无干扰；

3　执行这些功能的可靠性能力满足预期；

4　有充分的文档对执行这些功能的要求进行了描述。

5.3.7　应对智能传感器所执行的最主要测量相关安全功能进行评测，以证明其满足整体安全要求规范和油气管道现场的应用要求，具体评测内容包括：

1　所规定的主要测量相关安全功能的精度和可重复性；

2　传感器实现测量输出的响应时间和适当的信号处理能力（根据适当的产品或行业标准定义，如采样率、时间延迟、上升时间、带宽、滤波特性等）；

3　涉及频域转换功能时，候选设备应在相关频率范围内表现出足够的增益和相位变化能力；

4　制造商所定义的传感器安全状态（如开关量的输出状态，模拟量的电流值等），以及在安全控制器的组态配置时是否按照该安全状态的定义要求执行了适

当的信号逻辑处理；

5.3.8　应对智能传感器的非安全相关辅助功能开展评测，以证明其不会对安全相关功能造成不可接受的负面影响：

1　应检查确认传感器制造商在产品研发阶段是否开展了相关分析，并从设计的角度采取了适当的避免或控制措施；

2　应检查或测试传感器的配置功能是否具有输入合法性判断的能力，并能够拒绝或提示非法输入数值或输入方式；

3　应检查传感器是否对配置的能力进行了控制，一般仅限于生产运行或校准相关简单参数配置；

4　应检查传感器的配置进入、配置参数得到适当防护，以避免无意、恶意或未经授权的修改；

5　应分析或测试传感器的非安全相关的通信功能，在执行通信时外部连接设备的正常或异常均不会对传感器造成负面影响；

6　应检查传感器是否存在非特定应用项目所必须的功能（也称之为多余功能，例如仅有模拟量信号输出需求的应用场景配置有 HART 通信），对 SIL1~SIL3 的安全应用，应分析这些多余功能是否可能对安全测量造成负面影响，对 SIL3 的安全应用，还应采用测试的方式证明；

III 环境适应性评测

5.3.9　应对智能传感器在油气管道应用的环境适应性开展评测，具体包括：

1　通过测试或检查相关报告、说明确认传感器能够满足油气管道所在区域的极限环境条件，包括在高原、极寒、极热等环境下的温度、压力、湿度、腐蚀、射线、电磁干扰等；

2　通过分析、测试或检查相关报告确认传感器能够在极端环境条件下具有满足制造商声称的可靠性能力，包括（寿命、长期稳定性等），并能够满足在特定应用项目中的功能安全需求；

3　传感器可能需要依赖特定的辅助装置（如机柜、伴热等）来满足环境适应性要求，应评测应用现场是否具备相应的安装或维护条件。

5.3.10　已有的历史使用经验可以作为环境适应性符合的重要证据。

Ⅳ 可靠性、可维护性和可测试性评测

5.3.11 制造商所提供的失效模式及失效率是否满足 GB/T 20438 要求，以及在安装、运行和维护过程中满足所达到这些失效率的前提或假设条件。

5.3.12 对于传感器冗余应用的情况（如 1oo2 或 2oo3 等），应开展共因失效分析，确定其满足制造商在研发或认证过程中所假设的共因失效因子。

5.3.13 应对制造商在安全手册等文件给出的传感器检验测试策略进行评测，确认检验测试方法和限定的最长检验测试间隔在应用现场的可操作性和可实施性；分析所提出的检验测试方法预期可达到的测试覆盖率水平。

5.3.14 应结合制造商提供的失效率、现场实际的检验测试方法、现场实际可能实现的平均维护时间（MRT）以及检测到故障后传感器的行为模式来开展传感器部分的 PFD_{avg} 或 PFH 计算，并判断其是否小于分配给传感器部分的目标失效量。

5.3.15 应检查传感器的诊断测试间隔，确认当硬件故障裕度为 0 时，仅当高要求和连续运行模式下诊断测试间隔和执行特定功能以获得或维持安全状态的时间总和小于过程安全时间时，对传感器声称的诊断覆盖率才可采信。

5.3.16 应分析传感器达到相应诊断能力的前提和假设，并确认应用现场的整个系统配置过程中满足了相应的要求。

5.3.17 应检查传感器及其相关的规程/手册中是否考虑了对检验测试的支持。

5.3.18 应在制造商的支持下，评估传感器安全相关部分的寿命限制组件（如电解电容），以便在设备的预期故障率可能表明使用寿命结束之前，为组件或设备更换提供依据。

Ⅴ 用户文档评测

5.3.19 应检查传感器是否配有安全的安装、使用和维护的说明书，一般以安全手册或用户手册的形式呈现。

5.3.20 安全手册应符合 GB/T 20438.2 的附录 D 和 GB/T 20438.3 的附录 D 中的要求，至少包含：

1 完整的版本信息；

2 主要功能，配置参数的具体影响，设备接口，上电期间的行为，电源中断期间的行为，失效影响等；

3 安全相关功能的失效模式和失效指示；

4　辅助和多余功能的完整描述，包括相关的配置方式，以防止干扰主要功能；

5　功能完整性要求，如通过自诊断检测硬件失效，以及在检测到失效时采取的措施；

6　设备的环境和健壮性限制以及寿命限制部件；

7　所有维修、操作程序及其相应的警告；

8　定期维护、校准和检验测试的要求。

Ⅵ 测试的要求

5.3.21　在以上评测过程中，除了检查制造商已经完成的内外部测试报告之外，可能会对传感器开展附加的测试验证，典型的测试方式包括：

1　传感器样品的功能、性能和环境适应性测试；

2　传感器样品的故障插入测试，确认自诊断的有效性和故障安全输出的合理性；

3　设备对超范围输入或故障输入的响应测试；

4　配置等辅助功能的测试，及其在异常时对于传感器安全功能的影响性测试；

5.3.22　如果开展附加的测试，测试记录或相关文档应满足如下要求：

1　测试的文档应包括确定被测试产品的精确版本；

2　应记录测试的功能（应包括测试程序、测试数据、预期测试结果和观察到的结果）；

3　测试的设计应针对预期应用，以证明设备的性能与应用要求（包括边际条件和例外条件）一致；

4　测试环境应能代表预期应用，或应记录可以接受偏差的原因；

5　应记录测试的依据，以解释为什么测试结果可以证明所需的内容。

6 评 测 报 告

6.0.1 评测负责人应在完成评测后及时编制评测报告。

6.0.2 评测报告应至少包括以下内容：

1 经评测可以使用传感器满足的最高 SIL 能力，及其可满足的油气管道应用场景，可运行的运行环境限值；

2 按照本标准的评测要求，记录适用于相应安全完整性的理由；

3 应确定评估工作的范围和适用性，包括特定目标应用（安全功能）及其系统的等级；或者采取了一个更高的等级来评估设备的情况；经过评估涵盖的候选设备，包括候选设备的精确标识，如产品名称、软件和硬件组件的版本号、配置以及与评估相关的任何其他组件或选项；

4 应对可能影响设备是否可接受、目标等级、失效模式和环境使用条件的关键功能和性能要求进行归纳总结。这些要求是后续选型设备的基准，如果出现了偏离，也应详细记录，以便用户做最终的判断；

5 应记录设备可实现的可靠性目标，包括单独或冗余配置情况；

6 应包括（或者具有参考途径，如果这些文件都可以参考获得）用于验证设备各开发阶段的所有文件，包括验证的策略和执行的测试；

7 应确定在使用该设备的所有限制条件，包括应启用或禁用的特定选项或次要功能，包括每个类别所需的特定参数设置；

8 应确定当传感器存在微小并不影响安全功能的变更情况下，评测仍然有效的依据，给出当存在变更时可以接受的条件或者需要开展附加分析或测试的内容；

9 应确定传感器制造商对该传感器的售后技术支持的能力和持续时间等；应将传感器支持应用现场的文档、图纸和工具等作为评测报告的附件保留；

10 评测所使用的设备，评测的有效期，参与人员及批准人员签字。

用词说明

为便于在执行本标准条文时区别对待，对要求严格程度不同的用词说明如下：

1　表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2　表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3　表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4　表示有选择，在一定条件下可以这样做的，采用“可”。

引用标准名录

本标准引用下列标准。其中，注日期的，仅对该日期对应的版本使用本标准；不注日期的，其最新版适用于本标准。

《电气/电子/可编程电子安全相关系统的功能安全 第1部分：一般要求》GB/T 20438.1

《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 20438.2

《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 20438.3

中国工程建设标准化协会标准

油气管道智能传感器安全完整性评测规范

T/CECS 02XXX-202X

条文说明

目　　次

1　总　则

1.0.2　本标准不适用于对油气管道智能传感器在研发设计阶段的安全完整性评测，研制阶段的评测参考 GB/T 20438 等标准执行。本标准所规定的评测除了满足传感器产品级的功能安全要求以外，还需要考虑其在油气管道领域的应用特性，包括应用环境、生产工艺和操作特性等。

1.0.3　典型的智能传感器包括压力变送器、液位计、温度变送器、气体探测器等。

3　基 本 规 定

3.0.1　本标准所规定评测包括采用检查、分析或测试等手段，包括检查已有的设计、测试或手册文件，分析所给的安全相关数据或参数，以及对传感器直接开展测试。

5　评 测 内 容

5.1.2　应遵循的标准除了功能安全要求的标准如 GB/T 20438 系列以外，还应明确给出产品应满足的产品标准、油气管道行业应用标准或其他测试规范；

5.2　评测目标的构建

5.2.1　智能传感器可能会执行多个功能，甚至多个测量功能，评测重点关注的是其中执行安全相关的测量功能，例如某液位计的主要安全功能是测量液位，但同时也可以实现对液体密度等测量，评测关注的时该液位计的液位测量部分的功能和性能。共因失效分析可以参考 GB/T 20438.6，除传感器之间的冗余外，还宜评测传感器在应用中是否可能存在与其他设备或系统之间的共因失效问题，确认其是否可以接受。

5.2.2　不同项目所形成的 SRS 详尽程度可能不同，例如一些 SRS 中可能会明确给出传感器的安全完整性要求，这些要求即是本标准所定义的主要评测目标，然而

一些 SRS 中可能仅给出了整个 SIF 的安全完整性要求，那么在执行评测目标构建时需要基于整体的 SIF 分解为适当的对传感器的要求。

5.3 评测的实施

5.3.5 在评价运行经验是否充分有效时，可以参考如下内容。

6 充分的运行时间宜根据工程判断逐个项目确定，难以有一个统一的标准，可以参考 GB/T 20438.7 的附录 D 或其他适当的统计学理论，结合不同安全完整性目标失效量数值来确定最低的统计运行经验时间；

7 从现场统计的角度，可能很难有效的区分发生的失效是随机失效还是系统性失效。

5.3.15 完整的分析需要考虑到控制器和执行器等其他组件的时间。

5.3.16 例如某些开关类传感器，对其诊断的实现必须依赖于控制器的应用组态。

5.3.19 设备的安全使用是指在设备的安装、配置和维护方式适当符合设备供应商提供的文档的情况下，满足应用中预期的安全目标；一般情况下这种说明包括安全手册和用户手册等。