ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 44988—2024

过程工业安全仪表系统在线监视要求

On-line monitoring requirements for process industry safety instrumented systems

2024-11-28 发布　　2025-06-01 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、中石化安全工程研究院有限公司、中国石油天然气管道工程有限公司、深圳中广核工程设计有限公司、国能(连江)港电有限公司、中控技术股份有限公司、上海辰竹仪表有限公司、浙江正泰中自控制工程有限公司、美卓伦仪表(常州)有限公司。

本标准主要起草人：熊文泽、党文义、卜志军、史学玲、黄步余、陆卫军、贾永、吕峰、黄美良、杨阳、周婷、陈军松、朱杰、张益南、张艾森、余和伟、董秀娟、闫炳均、孙向东、何湘杰、刘瑶、李秋娟、李麟、田雨聪、史威、钱群福、马欣欣、范咏峰、于世恒、孙文勇、朱明露、韩鹏、陈超、曹德舜、李玉明、黄庆卿、姜巍巍、刁宇、魏振强、孟邹清、相桂生、李志勇、杨绍军、陈祖志、周亮、任军民、靳江红、刘英杰、刘培智。

引　言

安全仪表系统(SIS)运行过程中,过程变量的准确性是决定安全功能能否正确执行的关键,而过程变量是否能够得到准确及时的传输和计算,取决于SIS本身的状态(例如是否故障)。SIS的高诊断覆盖率设计可以产生大量有用的状态信息,系统检维修相关的状态信息对于安全能力是否实现也至关重要,传统上这些信息对于用户没有得到直观的展示,用户无法确切地知道安全仪表的实际运行情况,例如某个报警是内部器件故障、通信故障还是其他原因,或者当前情况下的安全完整性能力是否仍然维持设计的要求。这对于安全操作是非常不利的,对SIS的管理也难以有效开展。特别是高危复杂应用的SIS,准确、实时地获取现场设备安全相关信息并采取适当的处理措施是保障安全运行的关键。

因此,利用数字化和网络化的技术实现SIS的状态监视是非常重要的,这包括安全传感器、安全控制器和安全执行器的设备状态以及整个安全功能回路的状态。

通过这些状态的获取、分析和展示,可以提升生产运行过程中的安全性和可用性。例如操作员可以在关键的SIS出现异常时采取相对正确的动作,或者在安全能力无法满足预期时得到预先的提示。

本文件是对SIS运行过程中的在线监视要求进行规范,包括对整个安全仪表功能(SIF)状态和单体设备的监视。

通过有效执行在线分析可以提升SIS生产运行过程中安全性和可用性。

通过本文件的制定,还可以对在线监视过程的标准化给出实现要求,包括:

——设备/SIF的安全感知数据定义;

——安全感知数据的传输;

——安全感知数据的分析和展示。

过程工业安全仪表系统在线监视要求

1 范围

本文件规定了过程工业安全仪表系统在线监视的内容及相应数据感知、传输、分析和显示的要求。

本文件适用于过程工业领域安全仪表系统的在线监视。

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 21109.1 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

GB/T 42456 工业自动化和控制系统信息安全 IACS组件的安全技术要求

GB/T 42457 工业自动化和控制系统信息安全 产品安全开发生命周期要求

3 术语和定义

GB/T 21109.1界定的以及下列术语和定义适用于本文件。

3.1

在线监视 online monitoring

在正常生产运行过程中，开展的状态、属性或能力的实时感知与分析。

3.2

SIS在线监视系统 SIS online monitoring system；SIS-OMS

对安全仪表系统的实时状态、故障情况和安全完整性能力进行在线监视并给出适当报警提示的系统。

4 缩略语

下列缩略语适用于本文件。

A/D：模拟/数字(Analog/Digital)

AI：模拟量输入(Analog Input)

AO：模拟量输出(Analog Output)

CPU：中央处理单元(Central Processing Unit)

DI：数字量输入(Digital Input)

DO：数字量输出(Digital Output)

ERP：企业资源计划(Enterprise Resource Planning)

ESD：紧急停车(Emergency ShutDown)

HFT：硬件故障裕度(Hardware Fault Tolerance)

I/O:输入/输出(Input/Output)
IP:网际互连协议(Internet Protocol)
MAC:介质访问控制(Media Access Control)
PFD_{avg}:要求时危险失效平均概率(Average Probability of Dangerous Failure on Demand)
PFH:危险失效平均频率(Average Frequency of Dangerous Failures)
SC:系统性能力(Systematic Capability)
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)

5 总体要求

5.1 在线监视设置要求

5.1.1 应在SIS运行过程中设置适当的在线监视功能,以对SIS的运行状态和安全完整性能力进行持续监控。

5.1.2 SIS在线监视的在线检测、数据采集、通信、分析、显示等功能应满足其特定的工艺和安全仪表系统的设计要求。

5.1.3 SIS在线监视系统应不影响SIS安全功能的正常执行,应在设置过程中避免共因失效。

5.1.4 SIS在线监视宜由SIS系统集成实现,或者在其他系统中实现或独立设置。

5.1.5 应基于SIS中每个SIF回路的过程安全时间,确定在线监视的响应时间要求;对于特定SIF的在线监视响应时间,应小于该SIF回路过程安全时间的一半。

5.2 在线监视的权限管理和分类展示

5.2.1 在线监视应具备权限管理能力,包括面向操作员、工程师、调试人员等进行分类。针对不同角色人员,应明确相应人员的信息获取和操作权限,包括监视、诊断、报警处理和修改等。

5.2.2 在线监视应能够同时实现对SIS静态信息的展示(例如安全仪表制造商信息、冗余结构、固有失效率等)和运行过程中的动态状态监视(例如诊断情况、降级情况、故障情况等)。

5.2.3 在线监视应具备分类展示能力,面向不同的现场人员提供差异性的监视内容和报警信息展示。

5.3 在线监视的基本流程

5.3.1 实现在线监视的基本流程是:确定在线监视的内容(见第6章)、感知数据的产生(见第7章)、感知数据的传输(见第8章)、设备/回路安全参数和实时状态分析(见第9章)、分类展示和报警(见第10章),具体见图1。

5.3.2 基于在线监视的分析结论,可开展相应的现场应急响应,并提出设计优化和再次开展风险评估等需求,这些内容由特定应用现场的安全管理规程决定,本文件不再给出细节规定。

注:在线监视作为一种技术手段,能将SIS运行过程中复杂的功能安全问题通过感知数据的获取、分析,清楚直观展示给运行维护人员、工程设计方等,至于在得到这些SIS的运行状态和提示建议之后的操作,是由最近一次整体危险与风险评估的结论、现场的特定管理规程并结合GB/T 21109.1的相关要求决定。

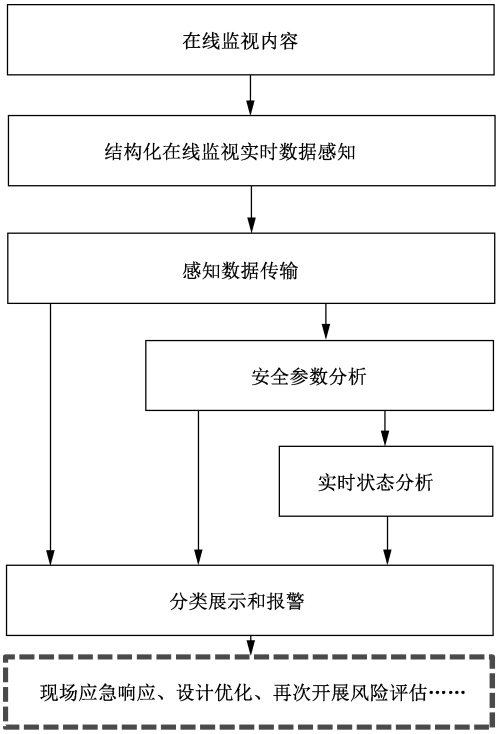

图 1　SIS 在线监视的实现框图

5.4　信息安全要求

5.4.1　SIS 在线监视系统应满足我国对工业自动化关键设施的信息安全法规和强制性标准的要求，包括信息安全等级保护中对工业控制系统的相关要求等。

5.4.2　SIS 在线监视系统应满足 GB/T 42457 和 GB/T 42456 的相关要求，同时功能安全和信息安全协同方面宜参考 IEC TR 63069 和 IEC PAS 63325 的要求。

5.4.3　SIS 在线监视系统在实现信息安全防护的过程中，应权衡保密性、完整性和可用性的要求。

6　在线监视的内容

6.1　通用要求

在线监视应能够实现对组件（包括传感器组件、逻辑控制器组件和最终执行元件等）和 SIF 回路的监视。

6.2　组件监视内容

6.2.1　应对组件进行监视，监视内容包括：

——基础信息，包括设备的类型型号、投运/停运信息、制造商、功能安全检测认证情况等；

——在用状态，包括处于正常运行、按要求执行了联锁动作、维修调试、旁路（强制）或停机等；

——实时故障情况，包括发生了何种故障、处于降级运行、故障运行等；

——自诊断情况，包括诊断有效性、诊断周期等；

——支撑组件安全功能执行的辅助设施状态，包括供电、供气等；

——操作情况，包括对该设备的操作信息、校准、维护、重启等；

——对该设备的维护信息，包括检验测试周期、预防性维护情况、日常巡检情况等。

6.2.2 基于在线监视的内容，应对以下信息进行历史记录留存，以便于后续的安全分析和设计完善，包括：

——每次故障记录，以及故障的详细内容：时间、位置、错误数据情况等；

——运行信息，包括投运/停运时间、运行在线和离线的时间等；

——操作维护情况，包括检验测试间隔、检验测试执行覆盖率信息等；

——要求间隔。

6.3 SIF 回路监视内容

应对 SIF 回路进行监视，监视内容包括：

——基础信息，包括 SIF 回路的编号、运行情况、联锁逻辑关系等；

——在用状态，包括处于正常运行、进入安全状态、旁路、强制或维修中等；

——实时故障情况，包括是否有 SIF 回路中的组件处于故障状态，降级状态等；

——维护情况，包括该 SIF 回路的检验测试频率、距离下次检验测试时间、检验测试执行覆盖率信息等；

——SIF 回路的硬件安全完整性情况，例如 PFD_{avg}、PFH、HFT 等；

——SIF 回路的安全相关特性，例如 SIL 等。

注：SIF 回路监视内容的信息来源可能是组成该回路的组件。

7 在线监视的数据感知

7.1 通用要求

为实现统一规范的 SIS 在线监视，产生结构化和规范化感知数据，对于数据感知应符合如下要求：

——实时获取表示组件或 SIF 回路状态的感知数据（见 7.2）；

——构建结构化的感知数据集（见 7.3）。

7.2 安全感知数据获取

7.2.1 可通过自动化或人工的方式获取开展在线监视所必须的 SIS 相关数据，为确保在线监视的及时性，应优先选用自动化的方式获取感知数据。

7.2.2 可通过多种渠道获取感知数据，典型的输入可来自：

——通过安全相关组件自身所提供的自诊断信息或状态信息（通过自诊断获取 SIS 状态信息的指南见附录 A）；

——通过外部现场设备或系统对 SIS 的附加监视信息（如环境温度、运行负荷等）；

——通过制造执行或管理系统（如 ERP）得到的 SIS 相关信息，例如运行维护的相关信息；

——人工录入的信息。

7.3 结构化安全感知数据集构建

7.3.1 安全感知结构化模型

应对感知获取的 SIS 安全相关数据构建结构化模型，以便于开展后续的分析和报警。

结构化模型所涉及的数据宜考虑到 SIS 所具有的安全相关属性，一般应至少包括如下属性：

——标识属性：SIS 在特定应用中的规定；

——安全属性：与安全参数直接相关；

——配置属性：对 SIS 开展配置相关的参数和架构信息等；

——过程属性：与过程测量和安全控制相关；

——运行维护属性：与 SIS 的操作、变更、维护活动相关。

基于 SIS 的实际现场应用，在每一类属性下面可继续构建下级属性，SIS 属性模型见图 2。

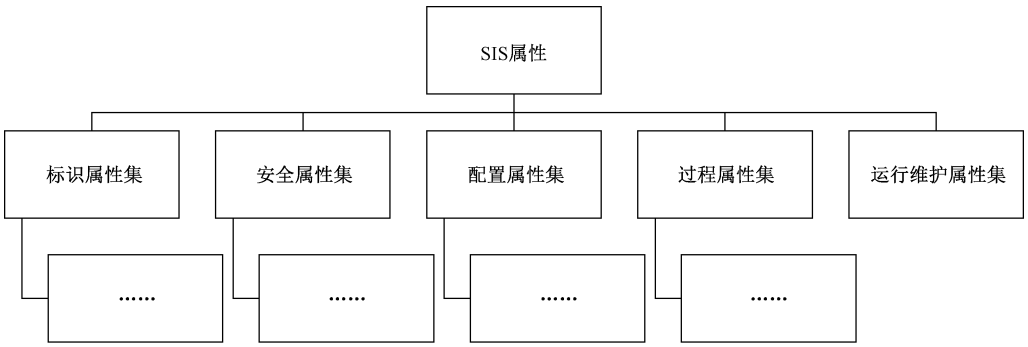

图 2　SIS 属性模型

在构建好的 SIS 属性基础上，应对每一下级属性建立结构化的数据集，形成 SIS 安全数据列表。一个属性模型及列表的构建示例见附录 B。

7.3.2　结构化的实现

应基于 SIS 属性，构建结构化的信息模型。结构化的实现过程可采用如下两种实现方式，两种实现方式见图 3。

——方式 1：在 SIS 内部单个组件内直接实现，例如在变送器内部直接构建安全数据列表，并将其传输给在线监视系统；

——方式 2：依靠外部转换模块完成，专用转换模块将安全组件内的非结构化数据转化为符合特定数据结构的安全数据列表。

注：对于实际的应用，标准化数据列表的生成不一定在安全设备本体，也可能采用专用的安全网关实现，但设备本体需提供足够的感知要素集，也就两种方式：

a）　安全相关设备在研制过程中即采用标准化数据列表；

b）　安全相关设备具有足够的感知要素集，但没有按照标准化数据列表格式，可能采用结合特定通信协议的转换网关，在网关处实现标准化安全数据列表的转化生成。

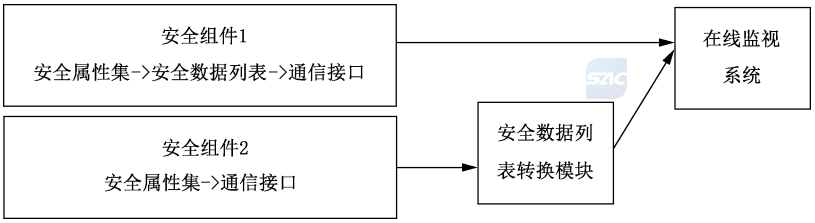

图 3　结构化安全感知数据的实现方式

8　在线监视的数据传输

8.1　通用要求

在线监视系统和受监视的 SIS 应具备数字化数据通信能力，以实现将在线监视数据的实时传输或

转移。

注 1：数据通信接口可能存在于现场仪表、控制器、上位机上，也可能存在于专用的在线监视平台上。

在线监视的数据传输可采用如下两种方式：

——传输方式 1：使用原有的 SIS 安全通信线路传输在线监视数据；

——传输方式 2：使用非 SIS 的其他通信线路传输在线监视数据。

注 2：以上两种方式可能在特定的在线监视应用中混合使用。

以上两种方式符合如下规定：

——数据传输应满足信息安全要求，见 5.4；

——应使用传输方式 1 的在线监视系统，其网络通信不影响安全仪表系统自身的控制命令和实时安全数据的传输，其指令集不与 SIS 控制指令混淆；

——宜根据安全仪表在线监视数据的变化频率和报告间隔要求，选择定期上传或查询两种通信方式，两种模式所带来的带宽开销不能影响原业务系统；

——数据传输应具备以下基本的可靠性能力：数据完整性的检查、数据丢失的检查、错序/乱序的检查和伪装的检查。

8.2 性能要求

8.2.1 若 SIS 在线监视系统采用传输方式 1，且 SIS 在线监视的通信系统程序独立于 SIS 系统软件部分，则在 SIS 线监视系统所占用峰值带宽不影响原安全通信功能的执行。

8.2.2 SIS 在线监视系统应保证通信的实时性，即通信数据在规定的时间内到达，整体时延应低于 3s，并具有超时报警的能力。

9 在线监视的数据分析

9.1 功能安全参数在线分析

9.1.1 在线分析系统基于传输的结构化安全实时数据，应至少执行如下在线分析：

——对故障的分析，以确保其失效率等参数持续满足设计阶段的验证计算假设；

——从投运开始总的要求率统计和产生要求的原因分析，以及是否满足危险与风险评估阶段的假设；

——误停车的频率和原因分析；

——自诊断能力的分析，包括自诊断的持续有效性，自诊断测试间隔时间，以及诊断到故障后系统的行为状态的合规性等；

——对检验测试执行情况的在线监视，包括检验测试的执行周期和检验测试覆盖率；

——对 SIF 降级运行的监视，降级运行的输出是否符合安全要求规范和安全手册，持续时间设计需求和 PFD_{avg}/PFH 的计算假设；

——关键的补偿措施（如泄压装置）涉及的设备的失效情况。

注：一些分析判断，需要基于该 SIS 在前期危险与风险评估和安全要求规范阶段的结论。

应基于以上分析的结论，对 SIF 的当前可实现 SIL 能力结论进行在线分析[SIF 实现特定 SIL 的要求可参考 GB/T 20438（所有部分）和 GB/T 21109（所有部分）]。

9.1.2 此外，还宜执行如下的在线分析：

——对安全仪表功能的操作是否符合安全设备的安全手册；

——基于长期故障统计的情况，对安全设备的失效率进行统计置信区间分析，并判断当前失效率数值的合理性；

——共因失效是否符合预期的实时分析（基于 GB/T 20438.6—2017 中的附录 D 中关于共因失效

因子的估算方法）；

——对 SIS 维护情况的分析，包括必要的预防性维护等；

——对故障后平均恢复时间的在线监视；

——每个 SIF 的 PFD_{avg}/PFH 的实时计算，以及是否仍然满足设计预期（如 SIL 目标）的判断；

——每个 SIF 中各个子系统 SFF 参数的实时计算，硬件故障裕度的实时分析；基于 SFF 和硬件故障裕度的各个子系统架构约束的实时分析，以及是否仍然满足设计预期的判断。

9.2 数据分析的安全能力要求

执行数据分析的模块应满足如下安全能力要求：

——满足功能安全要求，至少达到 SIL2；

——满足 5.4 的信息安全要求；

——至少按照 SIS 的检验测试频率执行功能完好性测试验证。

注：一个执行数据分析模块的例子是采用可靠性框图或马尔科夫模型的方式对硬件失效概率进行估算的运算模块。

10 在线监视的结果展示、报警

10.1 通用要求

10.1.1 应采用适当的方式展示在线监视的结果，并基于状态分析向运行人员给出明显的文字提示或声光报警。

10.1.2 应对所有 SIF 状态（系统回路级）和单个组件的状态进行分别展示、报警。

10.2 分类展示原则

对于现场的不同角色人员，可通过在线监视获得其所需的必要信息，典型的分类展示原则如下：

——宜向安全生产的管理人员直观的展示目前的整体的 SIF 统计状态及其 SIL 能力；

——宜向安全仪表系统的运行维护人员展示每一个设备/回路的安全参数和安全状态，并可直观的得到异常报警信息；

——安全仪表系统的设计人员宜获得设备/回路运行过程中详细的历史故障信息和联锁执行情况；

——安全仪表系统所属工艺装置的功能安全评估人员，宜获得详细的安全参数变化情况。

10.3 展示、报警内容

应至少对以下内容进行在线实时展示、报警：

——组件的关键安全参数，在超限时给出报警；

——是否发生 SIS 保护动作的指示；

——是否发生旁路保护功能的指示，并给出旁路报警；

——是否发生某个自动动作（如表决降级和/或故障处理）的指示，并给出报警；

——传感器和最终元件的状态，在异常时给出报警；

——影响安全的断电情况；

——组件的自诊断情况；

——支持 SIS 所需的环境调节设备的失效，并给出报警；

——SIF 的实时 SIL 能力，要求率情况，并在无法满足设计要求时给出报警；

——对 SIF 执行检验测试的情况，包括检验测试间隔的统计和检验测试覆盖率的结论，并在无法满足设计要求时给出报警。

10.4 数据统计

应对在线监视获得的故障统计原始数据进行存储，以便开展后续的安全分析，要求包括：

——应至少按照结构化数据的格式对故障数据进行统计，必要时可采取更加复杂的基于设备失效模式的统计记录方式；

——应在 SIS 在线监视系统的安装平台上预留足够的存储容量，以避免故障统计数据的溢出；

——应定期对统计数据导出备份，原则上备份周期不宜超过 1 年。

附 录 A
（资料性）
通过自诊断获取 SIS 状态信息的指南

A.1 SIS 组件的典型故障模式

为确保安全数据列表状态信息的有效实现，安全相关设备宜具有足够的状态自诊断/自监视能力，能够获得设备的测量、测量控制性能和状态信息，设备的设计宜能够诊断到特定故障、操作情况或性能异常，不同类型组件的典型故障模式如下。

a） 传感器子系统：

——温度仪表：仪表正常、传感器开路故障、传感器短路故障、超传感器极限故障、超量程上限故障、超量程下限故障、环境温度超限故障、电子部件故障；

——压力仪表：补偿数据校验错误、压力采样异常、温度采样异常、压力采样溢出、电子部件故障、A/D 标定数据校验错误、电流标定数据校验错误、板卡数据错误、压力超测量范围、电子部件故障；

——温湿度仪表：仪表正常、湿度传感器开路故障、湿度传感器短路故障、温度传感器开路故障、温度传感器短路故障、湿度超传感器极限故障、温度超传感器极限故障、湿度超量程上限故障、湿度超量程下限故障、温度超量程上限故障、温度超量程下限故障、环境温度超限故障、硬件故障、供电异常硬件故障、电子部件故障；

——雷达液位仪表：雷达故障、存储器故障、电流故障、温度故障、阈值过低、无有效回波；

——磁致伸缩液位仪表：电子模块温度低报警、电子模块温度高报警、主变量低报警、主变量高报警、子模块温度故障、参数异常故障、传感器故障、A/D 模块故障、恒流源故障、电子部件故障；

——可燃气体检测仪表：传感器故障、传感器离线故障、传感器超量程故障、自校准失败、分析通道故障、参考通道故障、控制器工作超温故障、备用电源充电过流或短路故障、主电源欠压故障、备用电源欠压故障、备用电源离线故障、探测器供电电源短路/过载故障、探测器超量程故障、探测器电流环信号与电源正极短路故障、探测器短路到电源负极或断路、电子部件故障；

——火焰检测仪表：火焰报警、传感器故障、控制器工作超温故障、备用电源充电过流或短路故障、主电源欠压故障、备用电源欠压故障、备用电源离线故障、探测器供电电源短路/过载故障、探测器电流环信号与电源正极短路故障、探测器短路到电源负极或断路、电子部件故障。

b） 逻辑解算器子系统：

——总体：系统故障、线路故障、超温故障、运行状态、强制状态、操作权限模式、CPU 负荷、通信负荷、降级运行、校时故障；

——供电单元：电源故障；

——控制单元：供电故障、模块/通道故障、总线故障、通信故障、运行故障、组态故障、超温故障、降级运行；

——通信单元：供电故障、模块/通道故障、总线故障、通信故障、组态故障；

——I/O 单元：供电故障、模块/通道故障、总线故障、组态故障、超温故障、采样点故障、输出点故障、线路开路、线路短路、外配电故障、采样点旁路、输出点旁路、降级运行、校时故障、超上限故障、超下限故障；

——安全栅：供电故障、线路开路、线路短路、超量程范围故障、精度超差故障、总线故障、通信故障、组态故障；

——继电器：供电故障、输入短路故障，输入开路故障、输入通道不平衡故障、触点粘连故障、逻辑故障、输出过压故障，输出过流故障。

c） 执行器子系统：

——电动执行机构：电池电量为空、负载力矩过大、关向力矩过大、开向力矩过大、电源相序检测错误、电机温度超过保护值、外接 380V 时手轮推入、执行机构运行超限、运行方向出错；

——电液执行机构：蓄能器压力报警、开阀超时报警、关阀超时报警、电机运行超时报警、ESD 报警、数据丢失、通信丢失时间、编码器故障、电磁阀电源故障、保压超时、补压超时、阀位超限、模拟信号丢失、限位设置故障、伺服无响应压力、传感器故障、动作超时、电机启动超时、活动实验超时、动力电源丢失、伺服告警阀位转向错、开阀超时、关阀超时、电机超时；

——气液执行机构：低电压报警、高电压报警、低电压报警、高电压报警；

——气动执行机构：断路器，电磁阀。

A.2 SIS 组件的典型诊断方法示例

为在运行过程中对组件进行持续状态监视，宜设计足够的诊断功能判断以上故障是否发生，安全相关组件的诊断可包括设备内部自诊断和外部诊断。

制造商宜描述其设备的内部自诊断能力，包括：

——诊断功能的参数和数值列表；

——标识方法，是否参数存储在现场设备上，用户是否可以设置以及如何设置；

——固定值或制造商默认的标准设定的详细信息。

在特定的工程应用中，可基于现场的实际情况配置如下外部诊断：

——附加在安全仪表系统上的额外外部诊断；

——其他系统对于与安全仪表系统相关的过程状态进行外部诊断；

——对于安全仪表系统周围环境状态，如温度、湿度、振动等情况进行的诊断。

典型的诊断措施设计方法见表 A.1。

表 A.1 诊断措施设计方法

序号	诊断方法	优缺点	示例
1	信号处理测试	简单且广泛使用的方法，但通常无法包括传感部分	通过写和读的操作来检查 A/D 和微处理之间连线的好坏
2	对测量参考变量的切换	包括传感部分，但是只能在特定的情况下中断功能来执行测试	在辐射测量中，对于参考脉冲的切换
3	使用参考信号	包括传感器部分，且无需中断正常功能	在重量测量中，增加一个额外的已知参考重量
4	使用测试信号，内部变量的变化情况	可包括执行和传感部分，但需要中断正常功能	检查信号周期性的定量增加是否符合预期
5	对参考信号的仿真	简单，但是一般仅用于补偿方法	测试信号用于具有力补偿的压力传感器

表 A.1　诊断措施设计方法（续）

序号	诊断方法	优缺点	示例
6	在现场增加额外的冗余传感器	多重的监视选项	例如浮子和微波测量互相比对
7	在现场增加额外的多样化传感器	可不用中断功能的执行，故障也可得到定位，但是仅能检测特定的某种故障，附加的传感器也增加了失效的可能	对于电容式单室差压传感器，电容值可转换为温度值，如果设置有另外一个温度传感器，通过比较两个数值就可确定膜片是否损坏
8	内部信号监视	可不用中断功能的执行，使用比较多	对于电容式液位测量，对电极之间的电流与参考进行比较
9	对于测量信息的理论和经验知识比对	可不用中断功能的执行，使用比较多	对处于晃动变化区域的流量计，通过对测量信号方差的监视可确定是否发生堵塞
10	运行情况的观测	不影响过程，诊断深度难以界定	对偏差、上升时间等进行监视

附 录 B
（资料性）
安全组件属性模型及列表构建示例

一个典型的 SIS 组件属性模型构建示例见图 B.1。

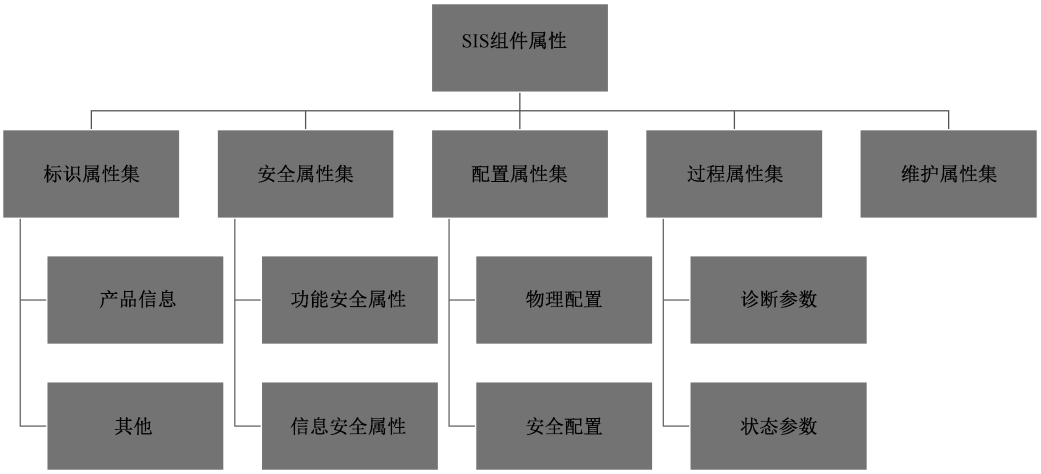

图 B.1 SIS 组件属性集构建示例

对以上 SIS 组件属性模型的详细属性列表示例见表 B.1～表 B.4。

表 B.1 标识属性集列表

类型编码及名称	子类型编码和名称	数值
0112/2///61987＃ABD885 产品基本信息	0112/2///61987＃ABA565——制造商	自定义
	0112/2///61987＃ABA567——设备名称	自定义
	0112/2///61987＃ABA566——设备类型	传感器子系统 逻辑控制器子系统 最终执行子系统 连接部件 网络安全部件
	0112/2///61987＃ABA581——产品编号	自定义
	0112/2///61987＃ABA300——产品代码	自定义
	0112/2///61987＃BAA022——现场位号	自定义
	0112/2///61987＃BAA023——安装地址	自定义
	0112/2///61987＃BAA034——投运时间	自定义
0112/2///61987＃ABC258 功能安全认可信息	0112/2///61987＃ABB081——功能安全评估认证文件	自定义
	0112/2///61987＃ABB953——功能安全评估认证机构	自定义
	0112/2///61987＃BAA028——功能安全评估认证有效期	自定义

表 B.2　安全属性集列表

类型编码及名称	子类型编码和名称	数值
0112/2///61987 ＃ABD877 功能安全属性	0112/2///61987＃ABA311——失效安全的方式	自定义
	0112/2///61987＃ABA313——预计服务寿命	自定义
	0112/2///61987＃ABB016——平均无故障时间	自定义
	0112/2///61987＃ABB202——安全完整性等级	1 2 3 4
	0112/2///61987＃ABA315——功能安全引用标准	自定义
	0112/2///61987＃ABB167——不能诊断到的危险失效率	自定义
	0112/2///61987＃ABB168——诊断到的危险失效率	自定义
	0112/2///61987＃ABB169——诊断到的安全失效率	自定义
	0112/2///61987＃ABB193——不能诊断到的安全失效率	自定义
	0112/2///61987＃ABB170——诊断覆盖率	自定义
	0112/2///61987＃ABB192——安全失效分数	自定义
	0112/2///61987＃ABB908——硬件故障裕度	自定义
	0112/2///61987＃ABB909——类型(A/B)	A B
	0112/2///61987＃ABB910——运行模式	低要求 高要求 连续
	0112/2///61987＃ABB911——检验测试周期	自定义
	0112/2///61987＃ABD735——检验测试方法	自定义
	0112/2///61987＃ABB018——内部冗余数量	自定义
	0112/2///61987＃ABB019——其他可靠性信息	自定义
	0112/2///61987＃ABA316——关键性代码	自定义
	0112/2///61987＃BAA001——诊断测试间隔	自定义
	0112/2///61987＃BAA024——最大响应时间	自定义
	0112/2///61987＃BAA025——检验测试覆盖率	自定义
	0112/2///61987＃BAA035——设备状态	自定义
	0112/2///61987＃BAA036——系统性安全完整性	1 2 3 4

表 B.3　配置属性集列表

类型编码及名称	子类型编码和名称	数值
0112/2///61987 #CAA002 物理配置	IP 地址	自定义
	MAC 地址	自定义
	可用资源情况(如内存等)	自定义
0112/2///61987 #CAA003 安全配置	访问控制规则	自定义
	流量过滤规则	自定义
	系统调用规则	自定义
	日志记录规则	自定义

表 B.4　过程属性集列表

类型编码及名称	子类型编码和名称	数值
0112/2///61987 #ABB597 设备诊断信息	0112/2///61987#ABN100——电路故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN101——断线	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN102——供电故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN103——信号丢失	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN104——传感器故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN107——通信错误	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABN108——微处理器故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#ABI407——其他	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA002—— 测量超限	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA003——AI 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA004——DI 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA005——DO 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA006——AO 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA007——PI 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA008——其他类型 I/O 模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA010——控制模块故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA011——通信故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA012——电源故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA013——线路故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA014——组态故障	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA029——安全联锁执行	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA015——驱动单元故障(如电磁阀、变频器等)	正常 1,故障后 0,不适用 NULL
	0112/2///61987#BAA016——执行单元故障(执行器、阀门、电机等)	正常 1,故障后 0,不适用 NULL

表 B.4　过程属性集列表（续）

类型编码及名称	子类型编码和名称	数值
设备状态信息	CPU 使用率	自定义
	内存使用率	自定义
	磁盘使用率	自定义
	网络通信速率	自定义
	越权调用	自定义
	非法网络连接	自定义
	运行状态	自定义

参 考 文 献

[1] 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

[2] 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

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

[4] GB/T 21109.2—2023 过程工业领域安全仪表系统的功能安全 第2部分:GB/T 21109.1—2022的应用指南

[5] GB/T 21109.3—2007 过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南

[6] IEC 61987 Industrial-process measurement and control—Data structures and elements in process equipment catalogues—Part 10: Lists of properties (LOPs) for industrial-process measurement and control for electronic data exchange—Fundamentals

[7] IEC TR 63069 Industrial-process measurement, control and automation—Framework for functional safety and security

[8] IEC PAS 63325 Lifecycle requirements for functional safety and security for IACS

[9] Mesch,F.Structures of automatic monitoring of measuring systems. Automatisierungs technische Praxis atp 43 (2001) H. 8, pp. 62- 67.