ICS
C

团　　体　　标　　准

T/CCSAS 0XX—202X

安全仪表功能（SIF）安全完整性等级（SIL）验证导则

Guidelines for safety integrity level (SIL) verification of safety instrumented functions (SIF)

（征求意见稿）

202X-XX-XX 发布　　202X-XX-XX 实施

中国化学品安全协会　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。

本文件由中国化学品安全协会提出并归口。

本文件起草单位：惠生工程（中国）有限公司、北京安必达科技有限公司、中国化学品安全协会、上海歌略软件科技有限公司、中科合成油工程有限公司、中国成达工程有限公司、中海壳牌石油化工有限公司、巴斯夫（中国）有限公司、珠海安彦企业管理咨询有限公司。

本文件主要起草人：程泱、唐彬、王琳、王楠、王娇龙、范咏峰、张红东、刘友玲、冯建柱、曾裕玲、代轶民、戴益、孙彦东。

安全仪表功能（SIF）安全完整性等级（SIL）验证导则

1 范围

本文件确立了安全仪表功能（SIF）的安全完整性等级（SIL）验证的原则，提供了验证原理、公式、示例、数据等内容；给出了失效率验证、结构约束验证、系统性安全完整性验证、验证程序、验证报告、验证审查等说明。

本文件适用于流程工业的SIL验证。

注：流程工业的含义见：GB/T 21109.1—2022 第1章 列项e。

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 20438.1—2017 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(IEC 61508-1:2010,IDT)

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(IEC 61508-22:2010,IDT)

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(IEC 61508-3:2010,IDT)

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(IEC 61508-4:2010,IDT)

GB/T 20438.5—2017 电气电子可编程电子安全相关系统的功能安全 第5部分：确定安全完整性等级的方法示例(IEC 61508-5:2010,IDT)

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/T20438.2和GB/T20438.3的应用指南(IEC 61508-6:2010,IDT)

GB/T 20438.7—2017 电气电子可编程电子安全相关系统的功能安全 第7部分：技术和措施概述(IEC 61508-7:2010,IDT)

注1：GB/T 20438 与 IEC 61508 最新版次相同，不再重复罗列。

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 61511-1:2016,IDT)

GB/T 21109.2—2007 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的应用指南(IEC 61511-2:2003,IDT)

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(IEC 61511-3:2003,IDT)

注2：GB/T 21109 与 IEC 61511 最新版次不同，再次罗列 IEC 61511 的最新版次。

GB/T 50770—2013 石油化工安全仪表系统设计规范

IEC 61511-1—2016(AMD 2017) Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements

IEC 61511-2—2016 Functional safety – Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1

IEC 61511-3—2016 Functional safety – Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required SIL

IEC 61511-4—2016 Functional safety – Safety instrumented systems for the process industry sector - Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

ISA TR84.00.02—2022 安全仪表功能的安全完整性等级（SIL）验证 (Safety integrity level (SIL) verification of safety instrumented functions)

ISA TR84.00.04—2020 第1部分：ANSI/ISA-61511-1:2018的实现导则 (Part 1 Guidelines for the implementation of ANSI/ISA-61511-1:2018)

ISO TR12489—2013, 石油、石化、天然气行业 – 安全系统的可靠性建模和计算 (Petroleum, petrochemical and natural gas industries -- Reliability modeling and calculation of safety systems)

3 术语和定义

GB/T 21109、GB/T 20438、IEC 61511、IEC 61508、ISA TR84.00.02中界定的以及下列术语和定义适用于本文件。

3.1

安全仪表功能 safety instrumented function (SIF)

由安全仪表系统SIS实现的安全功能。

注1：每个SIF实现要求的SIL，SIL定级与参与同一危险降低的其他保护层有关。

注2：来源：GB/T 21109.1—2022,3.2.66，有修改。

3.2

安全完整性等级 safety integrity level (SIL)

分配给 SIF 的分级（4 级)，明确安全仪表系统 SIS 实现的安全完整性要求。

注1：SIL等级越高，导致危险事故的PFDavg和PFH越低。

注2：目标失效范围与SIL等级之间的对应关系详见GB/T 21109.1—2022中的表4和表5。

注3：SIL4为最高级，SIL1为最低级。

注4：本定义与IEC61508-4—2010不同，反映了过程行业的不同。

注5：来源：GB/T 21109.1—2022,3.2.69，有修改。

3.3

验证 verification

通过检查和提供客观证据，确认要求已满足。

注1：SIL验证是SIS验证的一个环节，本文件的范围是SIL验证。

注2：来源：GB/T 21109.1—2022,3.2.87，有修改。

3.4

硬件故障裕度 hardware fault tolerance (HFT)

出现（硬件组件）故障或错误时，（硬件）功能单元继续执行要求功能的能力。

注1：HFT=1 表示：当多个组件中的1个故障时，单元可以工作。

注2：2oo3配置的危险故障的HFT是1；1oo3的是2。

注3：来源：GB/T 21109.1—2022,3.2.21，有修改。

3.5

系统性能力 systematic capability (SC)

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~SC4）。

注1：系统性能力由用于避免和控制系统性故障的要求来确定（见GB/T 20438.2和GB/T 20438.3）。

注2：相关的系统性失效机理取决于组件的特性。比如一个组件单独由软件构成，则只需考虑软件失效机理。如组件由硬件和软件构成则需要考虑硬件和软件的失效机理。

注3：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，组件具有SC N的系统性能力意味着SIL N的系统性安全完整性已被满足。

注4：来源：GB/T 20438.4—2017,3.5.9；GB/T 21109.1—2022,3.2.81。

3.6

要求时的平均失效概率 average probability of failure on demand (PFDavg)

在规定时间段内，当要求时，设备（系统）不能响应的平均概率。

注1：本文件中，PFDavg也可简写为PFD。PFD是时间的函数PFD(t)，通常使用时间段内的平均值。

注2：对于SIS，需求时，不能响应，即为危险故障。

注3：来源：ISA TR84.00.02—2022，附录B，有修改。

3.7

每小时的失效概率 probability of failure per hour (PFH)

每小时设备（系统）故障的平均次数。

注1：此处故障指危险故障。

注2：来源：ISA TR84.00.02—2022,7，有修改。

3.8

误停车率 spurious trip rate (STR)

在单位时间内，设备误动作引起的，工艺停车或混乱的预期次数。

注1：$STR = 1 / MTTF_{SP}$

注2：来源：ISA TR84.00.02—2022，附录B，有修改。

3.9

检验测试间隔 test interval (TI)

2 次成功的检验测试之间的时间间隔。也称为检测周期。

注1：本文件中，PTI proof test interval和TI含义相同。

注2：来源：ISA TR84.00.02—2022,7，有修改。

3.10

失效率 failure rate（λ）

时间点t之后的时间段dt内发生失效的设备总量，与t时间点完好设备的总量的比值，在dt趋向0时的极限值。

注1：本术语主要应用于随机失效。本文件假定设备中失效的数量相对于完好的数量，按固定比例出现。

注2：单位通常是FIT(10^{-9} 次/小时）。

注3：本术语应用于系统失效时，表示非设备自身原因导致的失效。

注4：来源：ISA TR84.00.02—2022，附录B，有修改。

4 符号和缩略语

下列符号和缩略语适用于本文件。

4.1 符号

M——N 取 M（MooN）表决配置中的 M。

N——N 取 M（MooN）表决配置中的 N。

R——N 取 M（MooN）表决配置中，R=N-M+1。例如：3 取 2 时，M=2，N=3，R=2。

β——共因因子。

λ——失效率。

μ——维修率。

4.2 缩略语

AC：结构约束（Architecture constraint）。

CCF：共因失效（Common caused failure）。

DC：诊断覆盖率（Diagnostic coverage）。

DI：诊断周期（Diagnostic interval）。

DR：需求率（Demand rate）。

DTT：非励磁停车（De-energize to trip）。

ETT：励磁停车（Energize to trip）。

FIT：菲特（Failure in time）。

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

FTA：故障树分析（Fault tree analysis）。

HFT：硬件故障裕度（Hardware fault tolerance）。

IF：独立失效（Independent failure）。

IPL：独立保护层（Independent protection layer）。

LOPA：保护层分析（Layer of protection analysis）。

MT：使用期限（Mission time）。

MTBF：平均失效间隔时间（Mean time between failure）。

MTTF：平均故障前时间（Mean time to failure）。

注1：也称为：平均无故障时间。

MTTR：平均恢复时间（Mean time to restore）。

PFDavg：要求时的平均失效概率（Average probability of failure on demand）。

注2：也称为：要求时的平均危险失效概率（Average probability of dangerous failure on demand）。

PFH：每小时的失效概率（Probability of failure per Hour）。

注3：也称为：每小时的失效概率（危险失效平均频率），Probability (average frequency of dangerous failures) of failure per hour。

PHA：工艺危害分析（Process hazard analysis）。

PTC：检验测试覆盖率（Proof test coverage）。

PVST：部分阀门行程测试（Partial valve stoke test）。

RRF：危险降低因子（Risk reduction factor）。

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）。

SRS：安全需求规范（Safety requirements specifications）。

SC：系统性能力（Systematic capability）。

STR：误停车率（Spurious trip rate）。

TI：检验测试间隔（Test interval）。

4.3 标志符号

在代码或缩略语上加标志，可构成新的含义。例如：λ_{DU}表示“危险、未检测到的失效率”。使用标志时，可用作下标、上标、尾缀，需保证可辨识、无歧义、统一。

应用于PFD、PFH、STR的标志如下：

- cal——计算值（Calculated）；
- FE——最终元件部分（Final element）；
- LS——逻辑解算器部分（Logic solver）；
- S——传感器部分（Sensor）；
- SS——支持系统部分（Supporting system）；
- tar——目标值（Target）。

应用于λ、MTTF的标志如下：

- D——危险、检测到的（Dangerous）；
- DD——危险（Dangerous detected） ；
- DU——危险、未检测到的（Dangerous undetected）；
- F——系统（Systematic）；
- S——Safe（安全）；
- SD——安全、检测到的（Safe detected）；
- SP——误停车（Spurious trip）；
- SU——安全、未检测到的（Safe Undetected）。

5 概述

5.1 SIL验证的外部工作关系见图1。

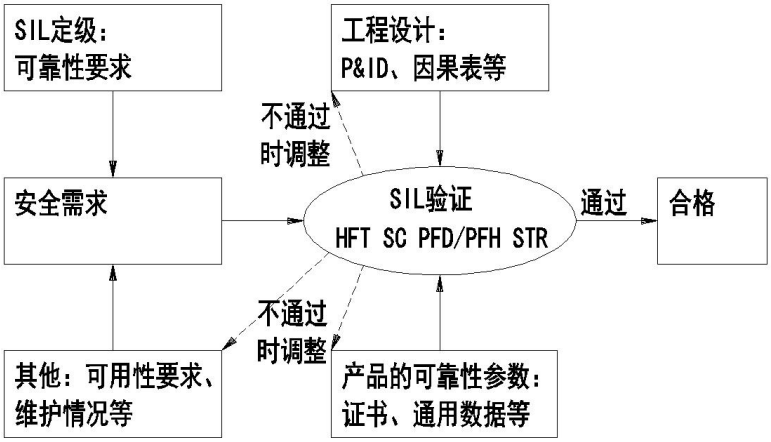


图1 SIL验证的外部关系

5.2 SIL验证可用于设计阶段的初步SIL验证、采购后的SIL验证、现有装置的SIL验证等。

5.3 SIL验证的输入（图1中实线箭头）为：

a) SIL定级：包括每个SIF的说明和SIL要求等；
b) 可用性要求：包括STR等参数；
c) 维护情况：包括TI等参数；
d) 产品参数：包括λ等参数；
e) 工程设计：包括P&ID、因果图等文件，用于方便理解验证对象。

5.4 产品参数的来源包括：企业和行业的通用数据、产品的证书数据。在初步验证阶段，未采购产品，无产品数据，可采用通用数据。

5.5 SIL验证的内部工作（图1中椭圆）包括：

a) 4项检查：冗余度（HFT）、系统性能力（SC）、可靠性（PFD/PFH）、误停车（STR）；
b) 3项计算：PFD、PFH、STR。合称SIF计算。

注：STR为可选。

5.6 SIL验证的检查表见表1。

表1 SIL检查表

SIL	PFDavg 注 1、2	PFH 注 1、2	SC	HFT（结构约束 AC 检查，危险 HFT） GB/T 21109	 GB/T 20438 Type A	 GB/T 20438 Type B	冗余设置 GB/T 50770
1	$<10^{-1}$ $\geqslant 10^{-2}$	$<10^{-5}$ $\geqslant 10^{-6}$	1	0	HFT 0 SFF 0 60 90 99 100 %	HFT 1 0 SFF 0 60 90 99 100 %	可单一
2	$<10^{-2}$ $\geqslant 10^{-3}$	$<10^{-6}$ $\geqslant 10^{-7}$	2	0/1 注 3	HFT 1 0 SFF 0 60 90 99 100 %	HFT 2 1 0 SFF 0 60 90 99 100 %	宜冗余
3	$<10^{-3}$ $\geqslant 10^{-4}$	$<10^{-7}$ $\geqslant 10^{-8}$	3	1	HFT 2 1 0 SFF 0 60 90 99 100 %	HFT - 2 1 0 SFF 0 60 90 99 100 %	应冗余
4	$<10^{-4}$ $\geqslant 10^{-5}$	$<10^{-8}$ $\geqslant 10^{-9}$	4	2	HFT - 2 1 SFF 0 60 90 99 100 %	HFT - 2 1 SFF 0 60 90 99 100 %	不适用

SIL	PFDavg 注 1、2	PFH 注 1、2	SC	HFT（结构约束 AC 检查，危险 HFT）			冗余设置
				GB/T 21109	GB/T 20438 Type A	GB/T 20438 Type B	GB/T 50770

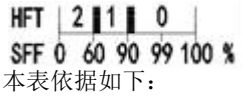
注 1：当 SIL 定级报告中有具体的 PFD 或 PFH 数值要求时，以其为准。

注 2：选择检查 PFD 或 PFH，取决于 SIF 的操作模式。操作模式的需求率决定了 PFD 或 PFH 更客观。

注 3：低需求模式时，为 0；高需求模式、连续模式时，为 1。

注 4：下图的含义是：0≤SFF＜60%时，为 2；60%≤SFF＜90%时，为 1；90%≤SFF≤100%时，为 0。其他类似。

SFF 的定义见图 6。



注 5：本表依据如下：

GB/T 21109.1—2022：条目 9.2.3、9.2.4、11.4、表 4、表 6。（PFDavg、PFH、HFT 依据）

GB/T 21109.1—2022：条目 3.2.80。（SC 依据）

GB/T 20438.2—2017, IEC 61508-2—2010：条目 7.4.4.2、7.4.4.3、表 2、表 3。（HFT 依据）

GB/T 50770—2013：条目 6.3、7.3、8.3。（参考的冗余依据）

注 6：STR 的检查依据为用户和项目要求。

5.7 组成SIF的组件设备的分类（Type A/B，表1中IEC 61508的分类）见表2。

表2 设备分类表

分类	条件
Type A	满足以下所有条件： 组成元件的失效模式可以清晰定义； 失效条件下设备的行为可完全确定； 有充足的数据说明可检测和不可检测危险失效率。
Type B	不满足以上条件之一。

5.8 验证报告的内容包括：输入整理、计算框图和过程、检查和结果、修改建议、相关产品证书等。示例见附录A。

5.9 当计算检查不合格时（图1中虚线箭头），需调整并重新计算检查直至合格。调整方法见附录C。

5.10 SIL验证结束后，结果可反馈至各上游工作中，形成闭环。

6 总体要求

6.1 SIF的SIL验证计算采用的仪表设备可靠性数据宜来自以往使用数据、SIL认证报告、公开发行的工业数据库或手册等。

6.2 用于逻辑控制器的可编程电子系统应取得国家授权认证机构的功能安全认证。

6.3 SIS或安全子系统的TI的确定应综合考虑SIL验证的符合性和企业检维修与停车的整体规划。SIS或安全子系统的TI宜与企业计划停车检修时间间隔相同。

6.4 为满足SIL验证的符合性，SIS或安全子系统的TI与企业计划停车检修时间间隔相同具有困难时，可采用不同的时间间隔。同一SIF的测量仪表、最终元件和逻辑控制器可采用不同的TI。

6.5 当安全仪表功能的误动作可能造成的损失大于可容忍程度时，可以规定可用性要求，并验证安全仪表功能满足可用性要求，如验证安全仪表功能的STR满足企业可用性要求。

6.6 SIF可用性冗余配置应满足法律、法规、规章、标准规范要求和企业可容忍风险标准的要求。在SIF的误停车不涉及法律、法规、规章、标准规范要求时，企业可决定误停车可容忍要求，并据此确定SIF的可用性配置。

6.7 同一个测量仪表、逻辑控制器、最终元件可以用于不同的安全仪表功能，共用部分应满足所有相关安全仪表功能的安全技术要求，包括仪表安全功能要求和安全完整性等级要求，并应进行验证。

6.8 SIS可执行非功能安全的仪表功能。SIS应具有优先权，非功能安全的仪表功能的失效或指令不应影响SIS的功能安全，包括不应降低SIF的安全完整性等级。

6.9 除非SIS紧急停车按钮和相关环节（包括操作人员和获取信息的措施）满足功能安全标准的要求并获得置信，SIS紧急停车按钮不应参与SIL验算，不应降低SIF可以达到的危险失效量。

6.10 SIL验证计算宜包括危险失效率（λ）、检验测试间隔（TI）、表决形式（MooN）、诊断覆盖率（DC）、平均恢复时间（MTTR）和共因失效因子（β）。

6.11 应确定SIF关键设备，SIF关键设备应参与SIL验证。非SIF关键设备不参与SIL验证。

6.12 SIF中的控制阀属于安全关键设备时，用于实现安全关键动作的控制阀的执行机构、电磁阀、阀体均应参与SIL验算。

6.13 石油化工工厂或装置SIF的SIL等级不应高于SIL3级。如果在确定SIL等级时，有可能达到SIL4，应重新分配保护层的安全功能，或采用多个独立的安全仪表功能，使SIL等级不高于SIL3。

6.14 应确定检测到故障时的系统行为，应确定对SIL验证的影响，检测到故障时的系统行为应符合GB/T 20438.2—2017的7.4.8的要求。

6.15 SIF有变动时，应重新开展SIL评估，含SIL定级、SIL验证。

6.16 SIL验证可建立全生命周期的动态机制，比如可根据仪表设备现场的实际运行情况，定期评估用于SIL验证的仪表设备的可靠性数据的合理性，如果发现用于SIL验证的仪表设备的可靠性数据不同于现场实际情况，可根据现场实际情况适当调整可靠性数据，赋值合适的失效率以符合现场实际情况，并开展SIL验证。

6.17 用于SIL验证的计算公式应符合现行的国家标准（GB/T 21109、GB/T 20438 等）、国际标准（IEC 61511、IEC 61508、ISA TR84.00.02 等）的要求。

7 过程和执行

7.1 验证程序

7.1.1 SIL验证节点

SIL 验证在多个节点开展，其中重要节点在 SIS 安全生命周期的 SIS 工程设计阶段开展，如图 2 所示。

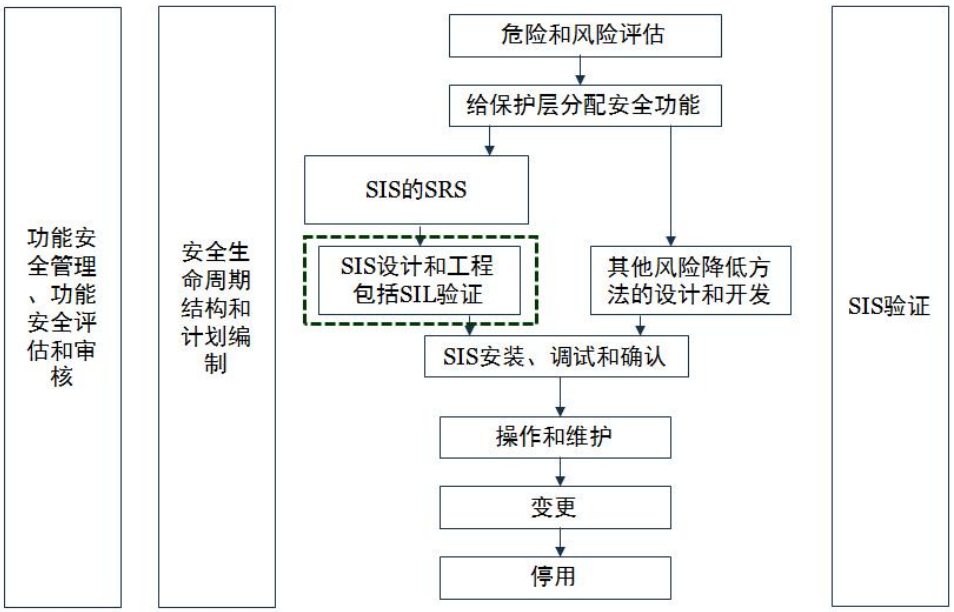


图2 SIS安全生命周期框图

7.1.2 SIL验证程序

典型的 SIL 验证流程如图 3 所示。

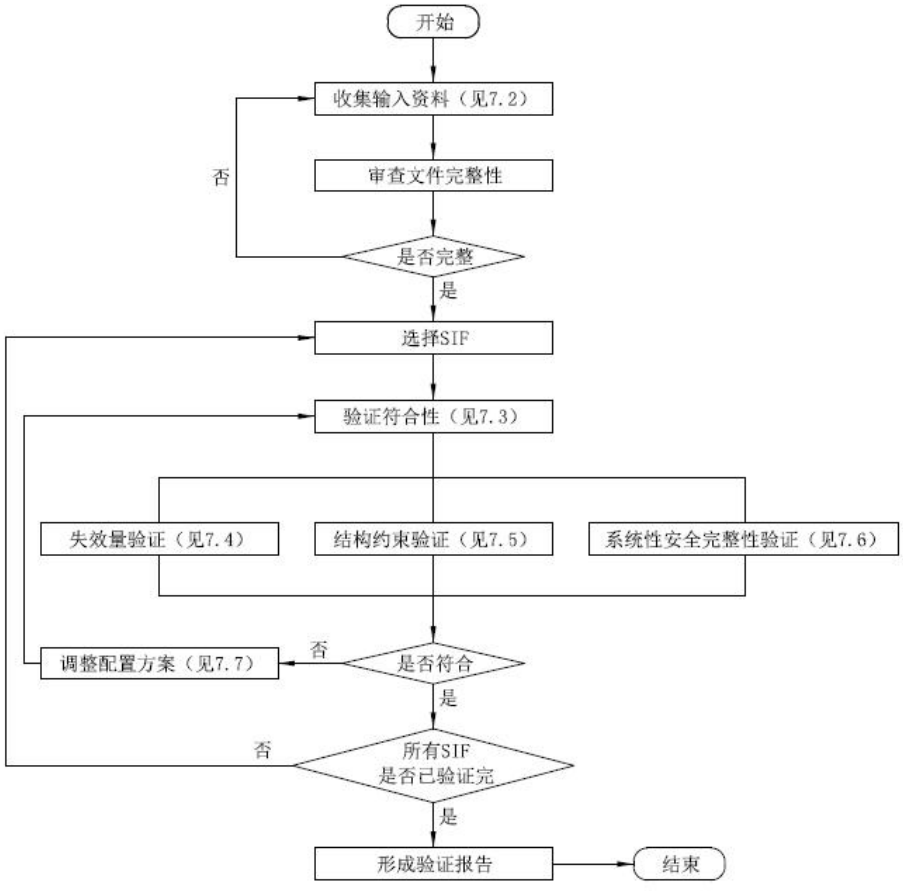


图3 SIL验证流程示意图

7.2 验证输入

7.2.1 SIL验证输入资料宜包括但不局限于以下资料：

a) 工程设计资料，包括 P&ID、逻辑图等；
b) SIF 清单、SIF 组成和 SIF 安全关键设备清单；
c) SIF 的 SIL 级别要求；
d) SIF 的操作模式；
e) SIF 的目标失效量要求；
f) 检验测试间隔（TI）；
g) 仪表设备的可靠性数据；
h) 配置方案，包括表决形式（MooN）；
i) 仪表设备安全手册。

7.2.2 可以检查表的形式检查SIL验证输入资料是否齐全，见附录B。

7.3 验证符合性

7.3.1 SIL验证应包括实施SIF硬件安全完整性验证；SIL验证可包括系统性安全完整性验证。

7.3.2 硬件安全完整性验证应包括失效量验证（见7.4）和结构约束验证（见7.5）。在低要求操作模式时，失效量验证应采用PFDavg验证；在连续操作模式或高要求操作模式时，失效量验证应采用PFH验证。

7.3.3 SC可用于系统安全完整性的验证，见7.6。

7.4 失效量验证

7.4.1 SIF应确定SIL等级要求。SIF宜确定明确的目标失效量。没有给出具体的目标失效量时，失效量应参考表3或表4，可采用要求达到的SIL等级对应的最小的平均失效率概率或失效频率。（参考GB/T 20438.1—2017 条目7.10.2.7 注1。）

7.4.2 SIF的计算失效量应不大于目标失效量。

7.4.3 在低要求操作模式时，SIF的SIL等级应采用PFDavg或RRF衡量，应根据表3确定。

表 3 安全完整性等级（低要求操作模式）

SIL	PFDavg	RRF
4	$\geq 10^{-5}$ 到 $<10^{-4}$	>10000 到 ≤100000
3	$\geq 10^{-4}$ 到 $<10^{-3}$	>1000 到 ≤10000
2	$\geq 10^{-4}$ 到 $<10^{-2}$	>100 到 ≤1000
1	$\geq 10^{-2}$ 到 $<10^{-1}$	>10 到 ≤100

7.4.4 在连续操作模式或高要求操作模式时，安全仪表功能的安全完整性等级应采用PFH衡量，宜根据表4确定。

表 4 安全完整性等级（连续操作模式或高要求操作模式）

SIL	PFH
4	≥10^{-9} 到 < 10^{-8}
3	≥10^{-8} 到 < 10^{-7}
2	≥10^{-7} 到 < 10^{-6}
1	≥10^{-6} 到 < 10^{-5}

7.5 结构约束验证

7.5.1 每个SIF均应满足结构约束的要求，结构约束要求可通过HFT的要求表达。

7.5.2 当SIS可被分解成独立的SIS子系统时（如测量仪表、逻辑控制器及执行元件），则HFT可在SIS子系统层级指定。

7.5.3 SIS或SIS子系统的HFT和相关要求应按照以下三种路线之一确定：

a) 符合表 5 的要求，并且全可变语言（FVL）和有限可变语言（LVL）可编程设备的诊断覆盖率应不小于 60%；

注1：此路线同GB/T 21109.1-2022中11.4.5～11.4.9建立的路线。GB/T 21109.1-2022中建立的路线源自GB/T 20438.2-2017中的路线2H。

b) 符合表 6 的要求和 GB/T 20438.2-2017 中 7.4.4.2（路线 1H）的要求；

注2：GB/T 20438.2-2017中的路线1H基于硬件故障裕度和安全失效分数的概念。

c) 符合表 5 的要求和 GB/T 20438.2-2017 中 7.4.4.3（路线 2H）的要求。

注3：GB/T 20438.2-2017中的路线2H基于由最终用户反馈的元器件可靠性数据、对指定的安全完整性等级增强的置信度和硬件故障裕度。

表 5 不同 SIL 对应的最小 HFT 要求

SIL	操作模式	要求的最小 HFT
1	任何模式	0
2	低要求模式	0
2	高要求/连续模式	1
3	任何模式	1
4	任何模式	2

表 6 安全相关组件或子系统执行安全功能时的最大允许安全完整性等级

组件的 SFF	HFT					
	A 类安全相关组件或子系统			B 类安全相关组件或子系统		
	0	1	2	0	1	2
＜60%	SIL1	SIL2	SIL3	不允许	SIL1	SIL2
60%～＜90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90%～＜99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4

组件的 SFF	HFT					
	A 类安全相关组件或子系统			B 类安全相关组件或子系统		
	0	1	2	0	1	2
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

7.6 系统性安全完整性验证

7.6.1 设备的系统性能力SC N应满足SIF要求的SIL等级要求。设备SC N的系统性能力是指SIL N的系统性安全完整性已被满足。

7.6.2 系统性安全完整性（系统性能力）要求，可通过实现以下合规路线之一来满足：

a) 路线1s：符合避免系统性工作要求（见GB/T 20438.2-2017的7.4.6和GB/T 20438.3）和控制系统性故障要求（见GB/T 20438.2-2017的7.4.7和GB/T 20438.3）；
b) 路线2s：符合设备以往使用证明的要求（见GB/T 20438.2-2017的7.4.10）；
c) 路线3s（仅针对已有软件组件）：符合GB/T 20438.3-2017的7.4.2.12的要求。

7.6.3 对于某具有系统性能力SC N（N=1，2，3）的组件，若该组件的系统性故障并不会使指定安全功能失效，而仅在另一个具有系统性能力SC N的组件同时发生系统故障时才会使指定功能失效，则在两个组件之间足够独立的前提下其组合的系统性能力可视为SC（N+1）。足够独立性的判断可参考GB/T 20438.2-2017的 7.4.3.4。

7.6.4 多个系统性能力为SC N的组件组合后可声明的最高系统性能力为SC（N+1）。每个SC N组件在这种方式下仅能使用一次，不允许继续增加SC N组件达到或超过SC （N+2）。

7.7 不合格调整

7.7.1 SIL验证不满足要求时，可采取的措施包括：

a) 选择高可靠性设备；
b) 提高冗余配置；
c) 缩短 TI；
d) 重新进行安全评估，考虑是否可以通过增加保护层来降低 SIL 等级要求。

7.7.2 调整配置对验证的影响示例见附录C。

7.8 验证报告

SIL 验证报告宜包括，但不局限于以下内容：

a) SIL 验证输入资料清单；
b) 说明硬件安全完整性验证的符合性；
c) 说明系统性安全完整性验证的符合性；
d) 说明 SIL 验证采用的公式，并说明标准符合性；
e) SIL 验证结果清单和建议清单。

7.9 验证审查

7.9.1 SIS开车前，应进行SIL验证审查。

7.9.2 SIL验证审查宜包括，但不局限于以下内容：

a) 审查 SIL 验证输入资料的有效性及是否齐全；
b) 审查 SIL 验证计算采用的公式是否符合功能安全标准的要求；
c) 审查 TI 的合理性；
d) 审查用于 SIL 验算的可靠性数据的来源；
e) 审查确定的仪表配置是否满足了 SIL 等级的要求。

7.10 验证示例

SIL验证的实例见附录A。附录A以实际的SIF为例，采用计算软件，详细具体的执行了SIL计算和验证。

a) 确认 SIF 功能回路的结构以及表决关系。根据最新版 SIL 定级报告中的 SIF 功能回路描述，确定回路中各个子系统涉及的各部件，如传感器子系统（输入）各部件、逻辑子系统各部件、最终执行元件子系统（输出）以及部件之间的逻辑表决结构。
b) 确认 SIF 功能回路各部件的失效数据。通过可信数据资料（现场使用积累数据，SIL 证书或可信数据库）等，确认该 SIF 功能回路内各部件硬件安全失效 SD/SU，危险失效 DD/DU 数据等。
c) 对于每一个子系统中的表决组，通过现场维护状态或可信数据资料，分析确认以下主要参数：
   - 选取的判断标准（本例中，使用 IEC 61511）；
   - 失效后果及响应模式（低，高或者连续）；
   - 预计部件的使用年限（MT）；
   - 检验测试间隔（TI）；
   - 检测覆盖率（PTC）；
   - 现场维护能力指数；
   - 共因失效因子等数据。
d) 计算 SIF 功能回路的要求时的平均失效概率 PFDavg 。使用相应计算软件计算 PFDavg 以及预期误动作率 STR(MTTFSP)。
e) 得到整个 SIF 功能回路的 PFDavg /HFT/系统性能力（SC），预期误动作率 STR(MTTFSP)后，参照标准确认 PFDavg 对应的 SIL 等级，其中 HFT/系统性能力（SC）（如适用）均满足要求，与定级时得到的 PFDavg（如适用）/SIL 比较，可判定该 SIF 回路是否实现 SIL 定级要求；如对误动作率 STR($MTTF_{SP}$)也有要求，同理可做比较判定。

8 方法和计算

8.1 概述

8.1.1 本文件中失效率通用数据和公式来自ISA TR84.00.02—2022。本文件主要罗列使用公式，次要说明使用公式的推导过程、假设前提、近似处理情况。

8.1.2 SIF计算的本质是通过现有的仪表可靠性，以概率数学的方式，在不同的维修方式下，预测SIF失效的概率、可靠性。其中的计算涉及仪表的可靠性数据管理、目标管理，以及有效的仪表供电、布线等安全设计。

8.1.3 SIF计算的内部过程见图4。依据设备的各类失效的概率，考虑逻辑结构、维护情况，计算系统的各类失效的概率。本图仅表示了主要部分，详细见后续章节。其中：计算输入见8.2；计算过程见8.3~8.7。

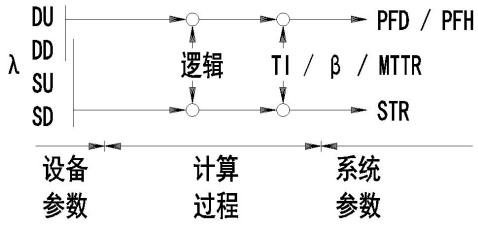


图4 SIF计算

8.1.4 PFD的整体计算过程如下。PFH、STR的过程相同。

1 个 SIF 包括 3 个部分：

a) 传感器部分：含传感器至解算器输入之间所有环节，通常包括变送器、安全栅等。通常需考虑 N 取 M 的结构、1 个 SIF 中涉及多个参数测量等因素。

b) 逻辑解算器部分：通常包括输入、控制器、输出、电源等。

c) 最终元件部分：含解算器输出至最终元件之间所有环节。通常包括阀体、执行机构、电磁阀、继电器等。通常需考虑多个阀门的关系、多个电磁阀的关系、部分行程测试等。

对于每一部分，从单体设备失效率，计算这部分子系统的 PFD。合并 3 部分求和,即 SIF 的 PFD。

8.2 失效的基本特征

8.2.1 本章节说明设备组件的失效。设备、组件等指组成系统、SIF的仪表、阀门、控制设备等。失效有时也称为故障。

注：关于失效和故障的定义和互换使用，参考GB/T 7826—2012 系统可靠性分析技术 失效模式和影响分析(FMEA)程序，条目3.3，注2。

8.2.2 失效的分级见表7。

表7 失效分级

失效分级	说明	举例
危险失效	因为设备故障不能完成设定的安全功能。	电磁阀卡顿：停车触发，电磁阀失电，但是电磁阀和阀门不动作。
安全失效	设备的误操作不会引起危险，或丧失保护功能。	电磁阀电缆断了，电磁阀失电，阀门误动作至停车触发的位置。

8.2.3 失效的模式见表8。

表8 失效模式

失效模式	说明	举例
完全失效	设备失去完成设定功能的能力。	需要时，切断阀不能全关。 工艺参数变化时，变送器信号无变化。 控制系统不能接受输入。
降级条件（部分失效）	设备的可靠性降低，仍能完成预设的功能，不满足预设的规格。 如果降级条件一直存在，会恶化为完全失效。 降级条件可以通过巡检、周期维护、预测性维护、诊断等发现，以防恶化。	控制输出高。 工艺参数指示高。 逻辑表决通道失效。
早期条件	不影响设备的功能。 如果不矫正，可能恶化为降级条件或完全失效。	接头松动。 端子腐蚀。 隔离被损坏。

8.2.4　失效的机理见表9。

表9 失效机理

失效机理	说明	举例
随机失效	本质原因是内部的。 随着时间而发生，可以预测。	变送器电路板故障。
系统失效	本质原因是外部的。 发生与时间无关，无法预测。依据经验整体估算，通过系统性的改善工作使之减少。	非常规的复杂的设计。复杂的诊断维护。不好的维护和操作。管理中的变更。 SIS 错误、接线错误、导压管错误、供气供电不足、安装错误、软件错误、人机接口错误、硬件设计错误、变更错误。

8.2.5　FMEA列表分析失效的模式、分级、原因、机理。例子详见附录I。

8.2.6　有些失效的根本原因是相同的，称为共因失效。非共因失效即独立失效。二者对于整个系统失效的影响是不同的。共因失效的占比是共用因子。

8.2.7　失效的详细分级见图5。

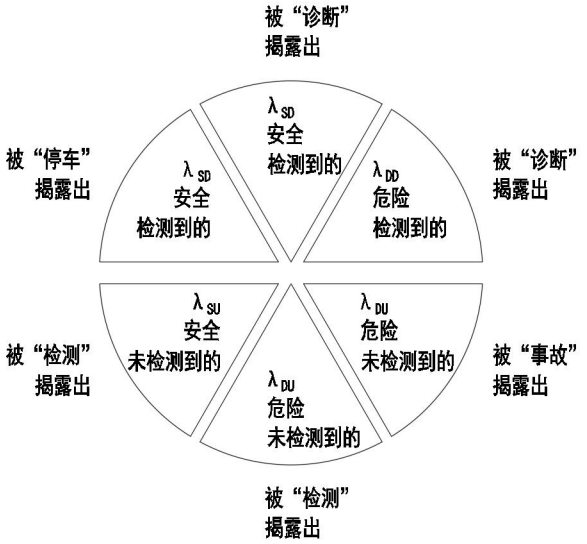
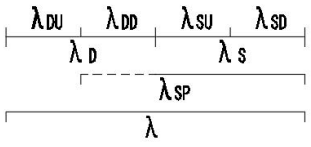


图5 失效详细分级

8.2.8 设备失效率的相关公式和示意见图6。



$DC = \lambda_{DD} / \lambda_D$ （需近似处理时：$DC = \lambda_{SD} / \lambda_S$ ）

$SFF = \lambda_{SP} / \lambda$

$\lambda = 1 / MTTF$

$MTBF = MTTF + MTTR \approx MTTF$ （MTTF远大于MTTR）

图6 设备失效率

其中：λ_{SP}是否包含λ_{DD}取决于系统设计，检测到的危险失效是否可以安全停车。通常认为失电停车DTT系统的λ_{SP}包含λ_{DD}；反之ETT不包含。

8.2.9 设备的失效率服从浴盆效应，见图7。早期，失效率高，主要是磨合失效；使用期，失效率稳定且低，主要是随机失效；末期，失效率高，主要是老化失效。SIL验证假设在使用期SIF的功能要求可靠运行，仅估算稳定期的随机失效率。

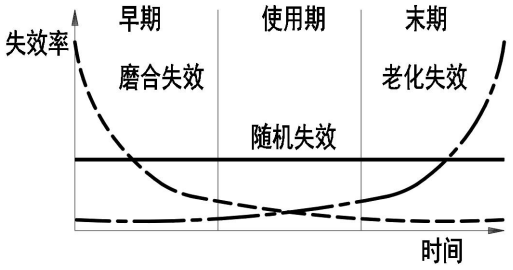


图7 浴盆效应

8.2.10 失效率数据的来源包括：企业的可靠性数据积累；行业数据手册和共享；制造厂SIL证书、安全手册等。SIL证书的数据需基于分析，可以查证。附录D罗列了一部分数据和来源。

8.3 操作模式

8.3.1 SIF的操作模式见表10。

表10 操作模式

操作模式	说明	举例
低需求模式	需求时，SIF 才动作。 DR≤1 次/年。	汽包液位低低： 作为保护措施，预期的 DR 为 0.1 次/年。
高需求模式	需求时，SIF 才动作。 DR＞1 次/年。	批量反应器进料超限： 每批次：16 小时运行，4 小时切换。每年：50 批次。DR = 600 次/年。
连续模式	SIF 是正常运行的一部分，使工艺处于安全状态。 SIF 的失效会导致危险的事故。	反应器温度： 温度控制必须维持正常；当超温时，其他手段（超温保护、超压保护等）因为具体原因（时间不足、措施不足等）不能保证反应器的安全。
DR = 需求次数 / 总操作时间。		

8.3.2 SIL验证的输入文件应明确每个SIF的操作模式，并明确验证值选择PFDavg或PFH。

8.3.3 PFDavg是1个时间段失效概率的平均值，PFH是瞬时值。选择依据是操作模式和DR（需求的频繁程度）。选择目的是更客观的反映实际情况。

8.3.4 STR的验证仅考虑瞬时情况，不考虑操作模式和DR。

8.4 PFH 计算

8.4.1 PFH的一般公式见（8-1）。

$$PFH_{NooM} = \frac{N!}{(N-M)!\,(M-1)!} \times (1-\beta) \times \lambda_D \times \left(\frac{(1-\beta) \times \lambda_D \times TI}{2}\right)^{N-M} + (\beta \times \lambda_D) \tag{8-1}$$

8.4.2 公式（8-1）的说明如下：

a) 本公式适用于 DR 较高的情况，包括：连续模式、需求模式（DR 较高时，通常是高需求模式）；
b) DR 较高时，诊断出的故障依然会导致失效，诊断对可靠性无贡献。因为：诊断出的危险失效没有时间将系统移至安全停车状态；
c) PFH 的计算基于 D 型失效，包括 DU、DD 型；DC 不参与计算。

8.4.3 PFH具体公式和推导见附录E。

8.5 PFD 计算

8.5.1 本条目详细说明PFD计算的原理和过程。PFH、STR的计算原理与PFD相同且简化，可不考虑时间积累等因素，因此PFH、STR计算各条目不再详述，参考PFD计算章节。

8.5.2 可靠性方块图是PFD计算的基本方法，它表示了组件和系统的失效传递关系。在图中有通路表示系统无失效，无通路表示系统有失效。

可靠性方块图（单表结构）见图8，3个部分的1个部分失效，无通路，整个系统失效，所以系统PFD等于组件PFD的汇总。

可靠性方块图（冗余结构）见图9，2个输入（S1/S2）组件中1个失效，有通路，这个环节没有失效。这个环节PFD不是2个组件的汇总，是基于排列组合的概率计算。

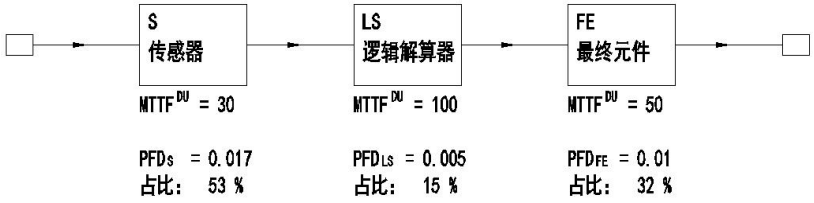


图8 可靠性方块图（单表结构）

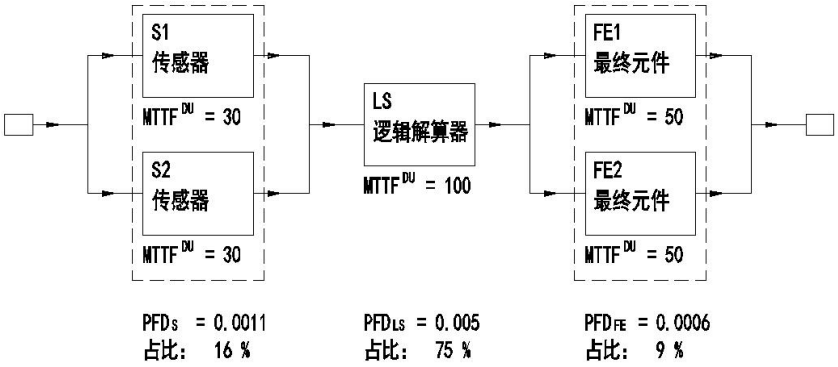


图9 可靠性方块图（冗余结构）

8.5.3 完整的维修时间应包括检测时间、准备时间、维修时间、等待延长时间，各部分见图10。实际应用中可忽略较小或未知的时间，并应明确MTTR。

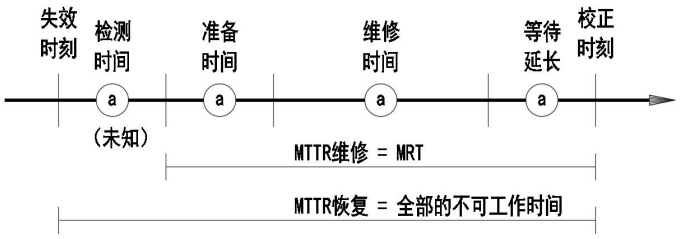
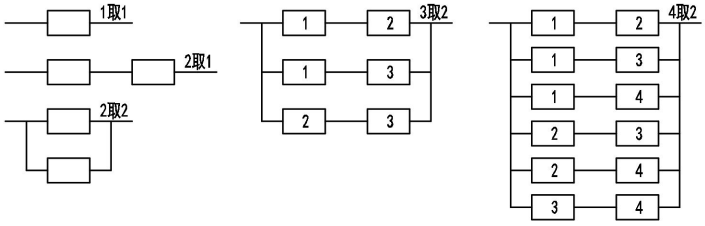


图10 MTTR

8.5.4 表决（N取M配置）逻辑影响了（单个仪表和组合之间的）失效传递关系，见表11。同一配置，对于危险失效、安全失效（误停车），这一传递关系是不同的。失效传递关系是建立模型的基础。

表11 表决

表决	危险 HFT	安全 HFT	逻辑图（危险失效的可靠性框图）
1 取 1	0	0	
2 取 1	1	0	
2 取 2	0	1	
3 取 2	1	1	
4 取 2	2	1	

8.5.5 共因抵消了冗余的作用。对于共因失效CCF部分，冗余配置无作用，相当于1取1（例：单表、单阀等）；对于独立失效IF部分，冗余降低了失效。示意见图11。

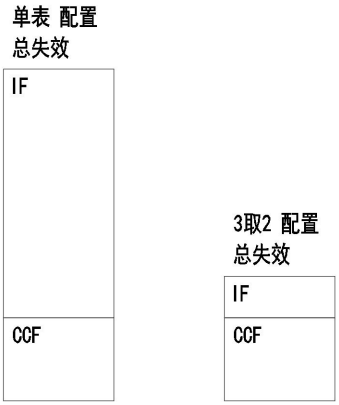


图11 共因

8.5.6 PFD基本公式的推导见附录E。故障树方法和马尔可夫方法的介绍，及PFD具体公式见附录F、G。

8.6 STR 计算

8.6.1 STR的一般公式见（8-2）。

$$STR_{MooN} = N!/(R!(M-1)!) \cdot R \cdot \lambda_{SP} \cdot (\lambda_{SP} \cdot (TI/2 + MTTR))^{M-1} \quad (8\text{-}2)$$

其中：

a) 假设共因失效少，可忽略。
b) 假设设备无连续自动诊断功能，检测时间为检修时间TI的一半。当设备为自动诊断功能时，去掉公式中的“TI/2”。
c) 公式推导为：冗余配置中，1个设备失效期间，另一个设备也失效的概率，并依次类推。

8.6.2 STR的具体公式见附录E。

8.7 SIF 计算

8.7.1 基于以下假设，可以把实际装置分析为理想化的模型，进而可开展SIF计算。

a) 设备的失效率和维修率在计算目标周期内是固定的；
b) 设备失效之后，修好之前，不会再次失效；
c) TI 远远小于 MTTF；
d) 测试和维修是完善的；
e) 所有设备选择正确。例如：阀门根据应用，在失效时都是安全位置；
f) 电源失效是非励磁状态；
g) 可检测的危险失效（DD）发生时，将发生安全停车；
h) 人员经过培训，按照制度工作。

8.7.2 SIF计算仅针对随机失效。系统失效部分无法定量计算，需整体处理。其代号为λ_F。

8.7.3 不同方法的SIF计算示例见附录H。

8.8 其他

8.8.1 冗余结构中，各个设备的失效率不同时，采用表12中的方法修改原公式。例如：采购不同制造厂的压力变送器组成3取2表决。

表12 不同失效率的公式调整

相同失效率 N取M	不同失效率 2取M	不同失效率 3取M
λ	$(\lambda 1+\lambda 2)/2$	$(\lambda 1+\lambda 2+\lambda 3)/3$
λ^2	$\lambda 1\lambda 2$	$(\lambda 1\lambda 2+\lambda 1\lambda 3+\lambda 2\lambda 3)/3$
λ^3		$\lambda 1\lambda 2\lambda 3$

8.8.2 SIF不等同于联锁逻辑，SIF号不等同于逻辑号。SIF指1个保护功能，1个SIF明确定义1个保护功能的范围和可靠性要求。逻辑用于定义因果关系，范围可调整大或小。1个逻辑号可涉及多个SIF号，也可反之，也存在二者一一对应的情况。

8.8.3 本文件未详细分析逻辑解算器的内部计算。可由系统厂家提供此部分的PFD、PFH和STR结果，直接使用。对于1个项目，结果可按类型复用。其计算原理类似传感器、最终元件的拆分。通常，逻辑解算器的PFD和STR在整个SIF中占比较小。表决信号的IO分配会通过共因，影响可靠性和计算。例如：3取2信号，分配至不同的IO卡，相比于相同的卡，可靠性更高，理论上PFD更低。

8.8.4 系统失效（例如：仪表合理选型、防止腐蚀、防止堵塞、仪表正确安装、回路失效安全搭建、维护水平等）对于SIF的可靠性影响很大，但是难以同随机失效（例如：变送器的λ参数、冗余配置）一样，通过SIF计算来体现。实际维护中，应通过减少系统失效，提高可靠性。

8.8.5 通过查表法计算PFD，可参考GB/T 20438.6(IEC61508-6) 附录B 条目B3.2.3。

8.8.6 PTC（检验测试覆盖率）对PFDavg的影响见图A.3。

当不全覆盖（PTC＜100%）时，会逐个提高MT内每个TI的PFD平均值。进而，第1个TI的PFD平均值，不等于整个MT（多个TI）的PFD平均值；当全覆盖（PTC=100%）时，两种平均值是相同的。尽量提高实践中测试的PTC，从而提高可靠性。

8.8.7 对于表决配置（当危险HFT＞0时，例：2取1、3取2等），β影响PFDavg，说明如下：

a) 对影响因素综合评分后，逻辑解算器的β取值分为4档：0.5%、1%、2%、5%，传感器和最终元件为：1%、2%、5%、10%；
b) 当参与计算时，β对计PFD的影响是正向的，即β越大，PFD越大；因为，β的部分内，各种表决降级为1取1（例：单表、单阀），消除了冗余降低失效的作用；
c) β受隔离、多样性、冗余、经验、工作文件化、维护制度、专业化、运行环境等多因素影响。典型的，不同测量方法、相同测量方法（不同制造厂）、相同测量方法（相同制造厂），3种情况：β的取值依次变大。最终元件的情况类似；
d) 尽量降低实践中的共因β，从而提高可靠性；
e) 参考GB/T 20438.6—2017 表D.4。

8.8.8 冗余结构中的硬件故障裕度，由SIL等级、需求模式、以往使用、故障安全、安全失效分数等共同决定。这些参数形成了子系统的结构约束。

8.8.9 “以往使用”的作法需要具备可靠性管理经验：对于在特定条件下使用的设备，经过评估，证明设备适合于操作条件，具有满意的检测、测试的方法，设备所在的安全仪表功能满足安全完整性等级要求。用户根据以往使用经验，汇总形成批准的供应商目录，有效管理可以使用在同一具体操作条件下的多个设备厂家和类型。同时用户建立自己的可靠性数据库，确定设备及其子系统的可靠性数据，通过可靠性目标管理，改善设备的维修方式和诊断方式，不断提高设备的可靠性，不断筛选证明合适的设备类型，提高SIF的安全完整性。

附录A
（资料性）
SIL验证示例

A.1 输入

本示例，使用软件，采用马尔科夫方法，对1个SIF进行SIL验证，结论为通过。

SIF 回路描述：贫胺液缓冲罐 D-01 液位 LT-01/02/03(2oo3)低低联锁，关闭贫胺液升压泵 P-01 出口 XV-01。

工艺过程描述：贫胺液经换热冷却进入贫胺液缓冲罐 D-01,再由缓冲罐出口贫胺液升压泵 P-01 升压进入循环氢脱硫塔。

SIF 功能：避免当循环氢脱硫塔循环氢（高压）通过贫胺液升压泵出入口倒窜入贫胺液缓冲罐 D-01，导致贫胺液缓冲罐超压爆炸着火。

定级要求：PFDavg＜1E-01 / SIL1。

工艺流程：见图 A.1。

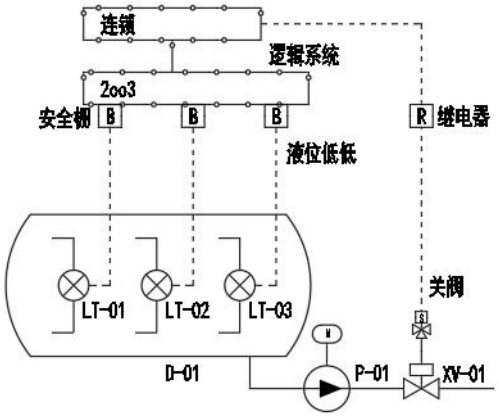


图 A.1 工艺流程

A.2 过程

搭建模型：该 SIF 功能回路结构分析如图 A.2 所示，分为测量单元，逻辑控制单元以及执行单元。为便于计算，测量单元包括引压管、传感器，信号转换和变送，安全栅以及浪涌保护器（如适用）等；逻辑控制单元包括 AI、AO、DI、DO、CPU 等模块；执行单元包括继电器或触点开关（如适用）、电磁阀（如适用）、执行机构和阀门等。

由图 A.1 可知，测量单元包括了三个液位测量仪表，LT-01/02/03，单元内表决关系为 2oo3，意即任意两个仪表低低报警即触发联锁动作；逻辑控制单元为 SIL3 认证的 SIS 系统；执行单元执行联锁动作，关闭一个阀门，表决关系为 1oo1。

图 A.2 SIF 结构

输入参数 整体部分：如下。

- MT = 10 年

- TI = 8760 小时（12 个月）
- PTC = 90%
- MTTR = 8 小时
- 失效后果及响应模式：低要求模式
- 现场维护能力指数：良好

输入参数 子系统部分：见表 A.1。

表 A.1 SIL 计算子系统的 SFF，β 以及 HFT

类型	SFF	β	HFT
测量单元	87.2%	5%	1
逻辑控制单元	97.8%	2%	1
执行单元	30.9%	0%	0

输入参数 组件部分：见表 A.2。

表 A.2 计算使用各组件的失效数据

子系统	位号	仪表类型	Type	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	数据来源
测量单元	LT-01/02/03	液位传感器	Type B	280	0	280	0	证书
		安全栅	Type B	280	0	280	0	通用数据
逻辑控制单元	SIS 系统	CPU 处理器	Type B	7430	75	2380	125	通用数据
		电源		2250	0	250	0	通用数据
		AI 模块		990	10	900	100	通用数据
		AI 通道		48	3	48	300	通用数据
		DO 模块		760	40	190	10	通用数据
		DO 通道		139	1	57	3	通用数据
执行单元	XV-01	继电器	Type B	0	900	0	600	通用数据
		电动球阀（整体）	Type A	0	600	0	5400	通用数据
注 1：λ的单位为 FIT（10^{-9} 次/小时）。 注 2：设备分类 Type 来自证书、通用数据。								

A.3 结论

计算和验证结论：通过。详细如下。

表 A.3 表示：各参数的计算结果，和要求值的对比。

图 A.3 表示：PFD 在使用年限内变化趋势，及其平均值 PFDavg。

图 A.4 表示：各子系统对整体的贡献比例。

表 A.3 SIL 计算结果汇总

目标 PFDavg / SIL 等级		＜1E-01/SIL1		
最终取得 PFDavg / SIL 等级		4.42E-02/SIL1		
	PFDavg	**$MTTF_{SP}$(年)**	**取得的 SIL**	
			SIL AC（IEC 61511）	**SIL SC**
SIF 回路整体	4.42E-02	38.59	2	1
测量单元	4.55E-04	499.81	3@HFT=1	1
逻辑控制单元	2.51E-05	287.91	3@HFT=1	3
执行单元	4.37E-02	48.93	2@HFT=0	1

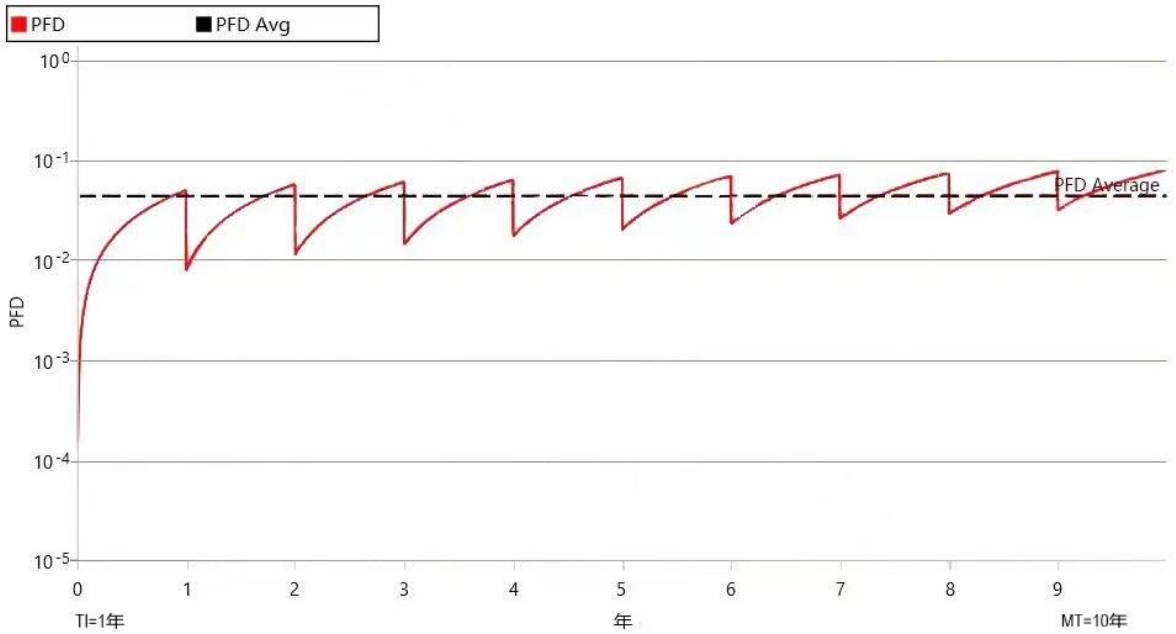


图 A.3 PFDavg 趋势图

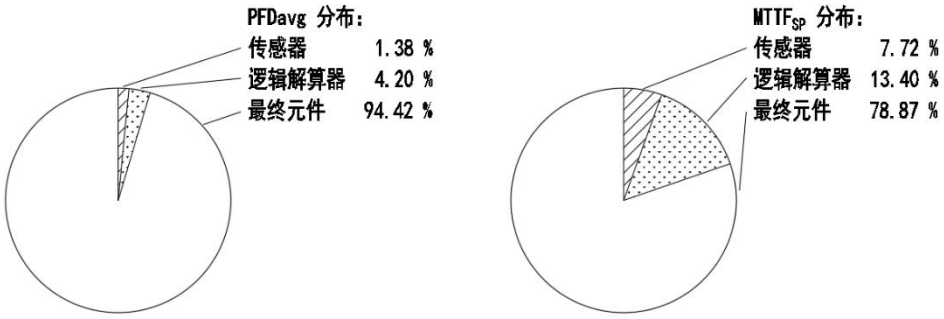


图 A.4 各子系统 PFDavg 和 $MTTF_{SP}$ 分布图

附录B
（资料性）
SIL验证输入

验证所需的输入文件和内容的检查清单，见表B.1。

表 B.1 SIL 验证输入清单

No.	输入文件	文件的内容	必须	补充	备注
1-1	SIL 定级报告（最新版）	SIF 清单	□		
1-2		SIF 组成	□		
1-3		SIF 安全关键清单	□		
1-4		SIF 的 SIL 级别要求	□		
1-5		SIF 的操作模式	□		
1-6		SIF 的目标失效量要求	□		
1-7		表决关系（MooN）	□		
2-1	仪表设备 SIL 证 或其对应型号的安全手册（注 1）	生产厂家	□		
2-2		仪表具体型号或系列	□		
2-3		失效数据	□		
2-4		SIL 等级（@HFT）	□		
2-5		SC 等级	□		
2-6		类型	□		
3-1	工艺 P&ID	设备以及仪表位号	□		
3-2		SIF 回路与工艺流程关系	□		
4-1	SIS 系统联锁逻辑说明与配置 或联锁逻辑图最新版（如适用） 或逻辑因果表（如适用）	SIF 配置方案		□	
4-2		表决关系（MooN）		□	
5-1	仪表规格书 仪表台账	生产厂家	□		
5-2		仪表具体型号或系列	□		
6-1	SIL 计算数据调研表（注 2）			□	
注 1：采取优先使用路径时，SIL 证书不是必须的。 注 2：可由业主填写，汇总测量仪表，逻辑控制器，执行元件等的信息。					

附录C
（资料性）
调整方法

验证不合格时的调整方法，见表C.1。

表C.1 调整方法

对象	动作	措施	可靠性 PFD/PFH	可用性 STR	经济性 成本	备注
共因	降低	采购不同制造厂的产品	提高	提高	不变	项目执行方便
		健全安全技术管理	提高	提高	不变	
	提高	采购相同制造厂的产品	降低	降低	不变	项目执行不方便
产品性能	提高	采购高档次的仪表	提高	提高	提高	
	降低	采购低档次的仪表	降低	降低	降低	
冗余结构	提高	1oo1、2oo2 改为 1oo2、2oo3	提高		提高	满足规范的要求
详见下条目	降低	1oo2、2oo3 改为 1oo1、2oo2		提高	降低	
冗余结构	提高	1oo1 改为 1oo2	提高	降低	提高	
		1oo1 改为 2oo2	降低	提高	提高	
		1oo1 改为 2oo3	提高	提高	提高	
		1oo2 改为 2oo3	降低	提高	提高	
		2oo2 改为 2oo3	提高	降低	提高	
	降低	2oo3 改为 1oo2	提高	降低	降低	
		2oo3 改为 2oo2	降低	提高	降低	
		2oo3 改为 1oo1	降低	降低	降低	
		1oo2 改为 1oo1	降低	提高	降低	
		2oo2 改为 1oo1	提高	降低	降低	
	修改	2oo2 改为 1oo2	提高	降低	不变	
		1oo2 改为 2oo2	降低	提高	不变	
部分行程测试	增加		提高	提高	提高	
	取消		降低	降低	降低	
检测周期 TI	缩短		提高	不变	提高	
	延长		降低	不变	降低	
MTTR	缩短		不变	提高	提高	
	延长		不变	降低	降低	

补充说明：针对验证不不合格的情况，还有其他应对策略。例如：考察该SIF设置的科学性和合理性。检查并分辨涉及安全的动作、安全无关的其他动作。

附录D
（资料性）
参考数据和来源

D.1　失效率的参考数据见表D.1、表D.2。

表D.1 常用失效率 仪表

	A公司		B公司		C公司		D公司		E公司		F公司	
MTTF单位：年	$MTTF^D$	$MTTF^S$	$MTTF^D$	$MTTF^S$	$MTTF^D$	$MTTF^S$	$MTTF^D$	$MTTF^S$	$MTTF^D$	$MTTF^S$	$MTTF^D$	$MTTF^S$
传感器												
流量开关			20-30	10-15	10	5	7	8	50	25	25	
压力开关			20-30	10-15	35	15	16	20	75	60	35	20
液位开关			20-30	10-15	25	5-10	80	60	100	50	30	60
温度开关			20-30	10-15	15	5	10	20	100	25	10	12
压力变送器	100	100	40-60	20-30	50	25	60	60	150	80	55	55
液位变送器	50	50	40-60	20-30	30	15	25	25	75	40	35	15
流量变送器									75	60		
孔板流量计	75	75	30-50	15-25	40	20	20	2	75	60	35	15
电磁流量计			40-50	20-25	100	25	150	150	75	40		
质量流量计			40-60	20-30	40	15	76		75	40		
涡街流量计			40-60	20-30	50	10			100	60		
温度变送器	75	75	40-60	20-30	40	20	160	100	200	23	65	50
火焰监测器	10000	1	15-30	5-15					30	24		
热电偶			60-80	30-40	40	20	20	10	200	23	100	20
RTD			60-80	30-40	30	15			150	40		
震动传感器	20	30	40-60	20-30	10	5			50	70		
可燃气体监测器									50	15	2.8	
最终元件												
气动闸阀	50	50	30-50	15-25	50	25	40	40	50	100	40	40
气动截止阀	50	50	40-60	20-30	60	25	40	40	50	100	40	40
气动球阀	50	50	40-60	20-30	50	25	40	120	60	150	40	40
电磁阀DTT	100	10	25-35	12-15	50	25	100	15	60	30	125	
电磁阀ETT	30	100							20			
电机启动器			1000-1500						761	229		
液动球阀							25	80	100	100		
电动球阀							15	135	15	134	30	
报警器							4	10	300	143		
电流开关			25-35						62	62		
继电器			1500-2500				70	40	500	400		
停车放大器									713	196		

表D.2 常用失效率 控制系统

项	低	典型	高
	失效率 1/百万小时		
主处理器板（内存、总线、通讯）	12.00	25.00	50.00
备用控制器	2.50	5.00	10.00
I/O处理器/通用I/O模块	2.50	5.00	10.00
单数字量输入电路	0.10	0.20	0.40
单数字量输出电路	0.10	0.20	0.40
单模拟量输入电路	0.05	0.10	0.20
单模拟量输出电路	0.25	0.50	1.00
继电器（工业型）	0.20	0.50	2.00
机电计时器	1.50	2.50	5.00
固态输入电路	0.10	0.20	0.40
固态输出电路	0.10	0.20	0.40
固态逻辑门	0.01	0.10	0.20
固态计时器	0.10	1.00	2.00
本质故障安全固态输入电路	0.05	0.10	0.20
本质故障安全固态输出电路	0.10	0.20	0.40
本质故障安全固态逻辑门	0.00	0.01	0.10
本质故障安全固态停延时计时器	0.05	0.50	1.00
模拟量停车放大器	0.10	0.20	0.40
电源	2.50	5.00	10.00
共因故障	无单位系数		
β	0.005	0.01	0.05
注1：数据来自制造厂。 注2：β值与失效率无关。例如：低失效率时，β值不一定是低或高。			

D.2 失效率数据的参考来源见表D.3。

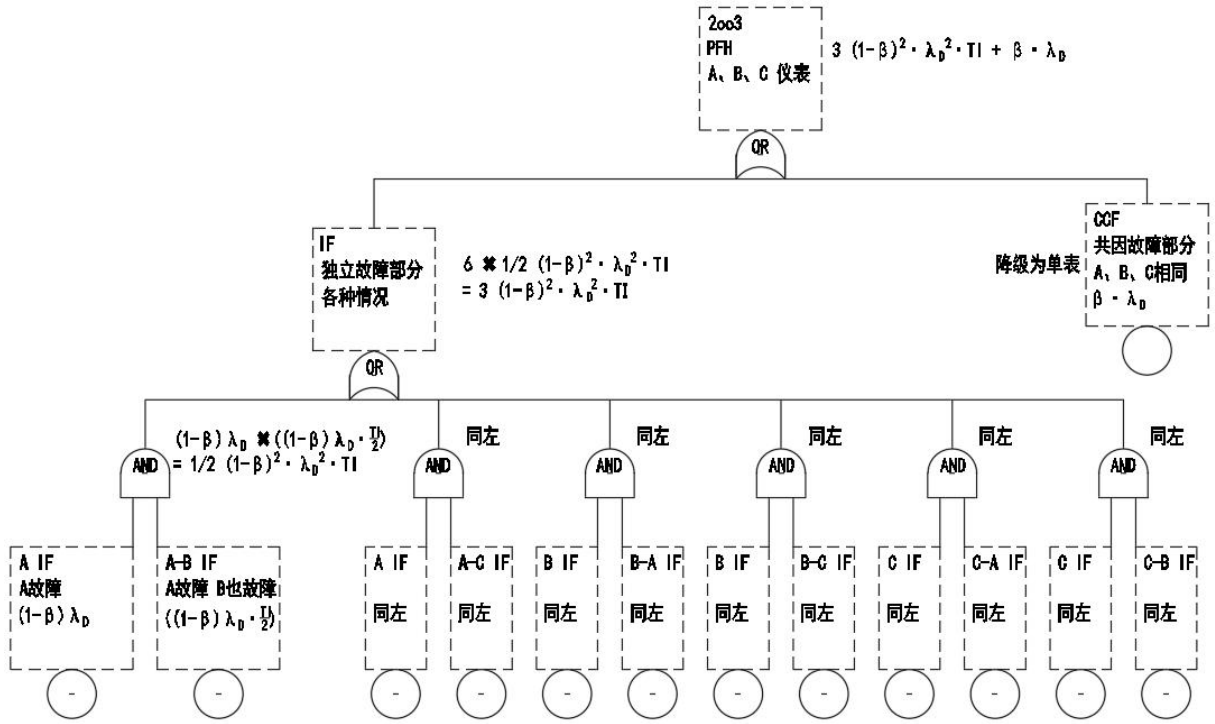
表D.3 数据来源

组织	出版物、手册	网址
PERD Process Equipment Reliability Database		http://www.aiche.org/CCPS/Active Projects/PERD/inde x.aspx
PDS Forum	PDS Data Handbook	http://www.sintef.no/Projectweb/PDS-Main-Page/
OREDA Offshore Reliability Data	OREDA Handbook	http://www.oreda.com
Instrument Reliability Network		https://irn.tamu.edu
WIB (International Instrument Users' Association)		http://www.wib.nl
IEEE	IEEE Standard 493	
RIAC	EPRD Electronic Parts Reliability Data NPRD Non-electronic Parts Reliability Data	

附录E
（资料性）
公式和推导

E.1 PFH公式推导、公式、计算实例

对于3取2配置，采用故障树模型，推导PFH公式。见图E.1。



图E.1 PFH失效模型

对于各种配置，推导的结果，见表E.1。

表E.1 PFH公式

配置	公式 STR
1取1	λ_{SP}
2取1	$2\ \lambda_{SP}$
3取1	$3\ \lambda_{SP}$
2取2	$2\ \lambda_{SP} \cdot (\lambda_{SP} \cdot TI/2 + \lambda_{SP} \cdot MTTR)$
3取2	$6\ \lambda_{SP} \cdot (\lambda_{SP} \cdot TI/2 + \lambda_{SP} \cdot MTTR)$
3取3	$3\ \lambda_{SP} \cdot (\lambda_{SP} \cdot TI/2 + \lambda_{SP} \cdot MTTR)^2$
注：公式的适用条件、参数调整见正文章节。	

计算例子的汇总见表E.2。计算过程略。

表E.2 PFH例子结果汇总

λ_D	0.05 / 年		0.008 / 年	
TI	1 年	5 年	1 年	5 年
1取1	0.05	0.05	0.008	0.008
2取1	0.0034	0.013	0.00022	0.00047
3取1	0.0011	0.0032	0.00016	0.00017
2取2	0.1	0.1	0.016	0.016
2取3	0.0082	0.037	0.00034	0.0011
3取3	0.15	0.15	0.024	0.024
注1：本表罗列24种情况：2种λ_D取值、2种TI取值、6种配置。 注2：β= 2% 。				

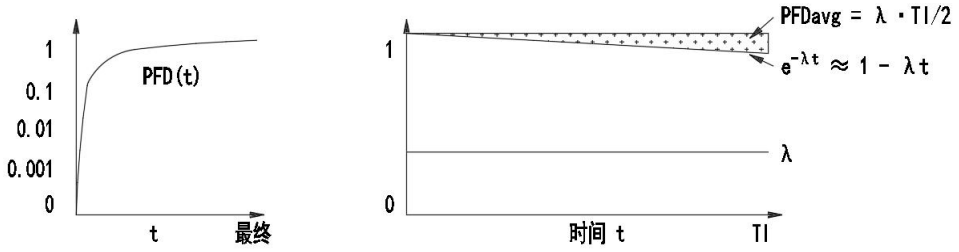
E.2 PFD基本公式推导

结论：对于单个设备，PFDavg =λ•TI/2

推导过程：见ISA TR84.00-02—2022 附录D。

说明：见图E.2。左图中，PFD是时间的函数。右图说明如下：

- 失效的比例是固定的。即：λ。
- 失效按比例发生。每个时刻，都基于目前的可靠总量，发生等比例的失效。通过微分并积分（本文件略去），可知未失效的可用数量是λ和时间的指数函数。即： $e^{-\lambda t}$。
- PFDavg是平均值，失效数量在TI周期（远小于最终寿命）内的积分并近似。即：PFDavg =λ•TI/2。



图E.2 PFD示意

E.3 STR公式

STR的公式见表E.3。

表E.3 STR公式

配置	公式 STR
1取1	λ_{SP}
2取1	$2\ \lambda_{SP}$
3取1	$3\ \lambda_{SP}$
2取2	$2\ \lambda_{SP}^2 \cdot (TI/2 + MTTR)$
3取2	$6\ \lambda_{SP}^2 \cdot (TI/2 + MTTR)$
3取3	$3\ \lambda_{SP}^3 \cdot (TI/2 + MTTR)^2$
注：公式的适用条件、参数调整见正文章节。	

附录F
（资料性）
故障树方法和PFD

F.1 说明

FTA故障树分析起源于10世纪60年代，在贝尔电话实验室，由H.A.Waston，用于估算北极星导弹项目的安全性，和民兵导弹误发射的可能性。70年代，扩展至核工业，用于估算核反应堆失控的可能性。80年代，扩展至流程工业，用于估算事故的可能性，包括SIF失效的可能性。FTA用于估算设备和组件失效导致事故的可能性，是公认的技术。

FTA需基于对估算对象（SIF设计）的正确理解。FTA不能替换SIF设计本身。FTA仅图示和罗列故障路径，估算总体失效。

FTA的计算基于底层设备组件的失效率，这些数据来自大量工业数据的积累，并需根据工艺操作条件、环境条件、操作经验、维护经验、设备年限等调整。

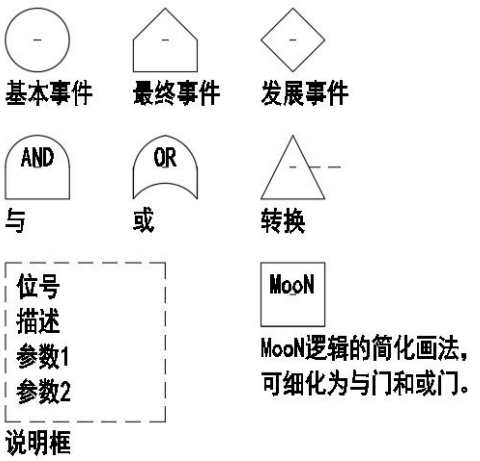
FTA完整的计算量非常大，可按需分层次采用近似的公式。

F.2 作业说明

FTA的工作步序见表F.1，采用的图例见图F.1。

表F.1 FTA步序

步序	说明
1	SIF 描述和信息：仪表、工艺、公用工程（仪表风、供电等）、检修周期（离线\在线）、失效模式、失效率、诊断、维修周期（离线\在线）、共因、系统失效。
2	顶端事件辨识：以 PFD（安全功能失效）或 STR（误停车）为目标的顶端事件。
3	构造故障树：从基本事件（设备组件各类失效）到顶端事件的逻辑传递关系。采用图 F.1 的图例。
4	定性检查故障树：需工艺和仪表的设计、操作、危险评估人员。
5	定量估算。



图F.1 FTA图例

F.3 公式

故障树法的PFDavg一般公式见F-1。

$$PFDavg = N!/(R!(M-1)!) \cdot ((1-\beta) \cdot ((1-DC) \cdot \lambda_D \cdot TI/2 + DC \cdot \lambda_D \cdot DI/2 + \lambda_D \cdot MTTR)^R + \beta \cdot ((1-DC) \cdot \lambda_D \cdot TI/2 + DC \cdot \lambda_D \cdot DI/2 + \lambda_D \cdot MTTR) \quad (F-1)$$

公式考虑了共因。对于CCF部分，冗余配置降级为1取1（无冗余），体现为公式中β系数的部分。对于IF部分，体现为公式中（1-β）系数的部分。

故障树法的PFDavg具体公式见表F.2。

表F.2 故障树法的PFDavg近似公式

配置	近似公式 PFDavg 故障树法
1取1	$(1-DC) \cdot \lambda_D \cdot TI/2 + DC \cdot \lambda_D \cdot DI/2 + \lambda_D \cdot MTTR$
2取1	$((1-DC) \cdot (1-\beta) \cdot \lambda_D \cdot TI/2 + DC \cdot (1-\beta) \cdot \lambda_D \cdot DI/2 + (1-\beta) \cdot \lambda_D \cdot MTTR)^2$ + $((1-DC) \cdot \beta \cdot \lambda_D \cdot TI/2 + DC \cdot \beta \cdot \lambda_D \cdot DI/2 + \beta \cdot \lambda_D \cdot MTTR)$
3取1	$((1-DC) \cdot (1-\beta) \cdot \lambda_D \cdot TI/2 + DC \cdot (1-\beta) \cdot \lambda_D \cdot DI/2 + (1-\beta) \cdot \lambda_D \cdot MTTR)^3$ + $((1-DC) \cdot \beta \cdot \lambda_D \cdot TI/2 + DC \cdot \beta \cdot \lambda_D \cdot DI/2 + \beta \cdot \lambda_D \cdot MTTR)$
2取2	$2 \cdot ((1-DC) \cdot \lambda_D \cdot TI/2 + DC \cdot \lambda_D \cdot DI/2 + \lambda_D \cdot MTTR)$
3取2	$3 \cdot ((1-DC) \cdot (1-\beta) \cdot \lambda_D \cdot TI/2 + DC \cdot (1-\beta) \cdot \lambda_D \cdot DI/2 + (1-\beta) \cdot \lambda_D \cdot MTTR)^2$ + $((1-DC) \cdot \beta \cdot \lambda_D \cdot TI/2 + DC \cdot \beta \cdot \lambda_D \cdot DI/2 + \beta \cdot \lambda_D \cdot MTTR)$
3取3	$3 \cdot ((1-DC) \cdot \lambda_D \cdot TI/2 + DC \cdot \lambda_D \cdot DI/2 + \lambda_D \cdot MTTR)$

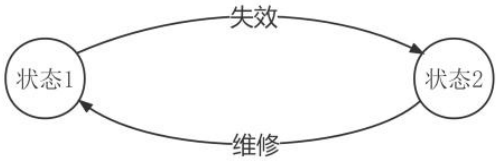
附录G
（资料性）
马尔可夫方法和PFD

G.1 说明

马尔可夫Markov模型或方法由苏联数学家A.A.Markov(1856-1922)提出。其致力于随机过程的数学分析，并得到了广泛的发展和应用。是定量分析SIS可靠性的方法之一。

马尔可夫模型包括系统状态和转换，状态之间的转换原因是故障和维修。状态转换以概率发生，并是下次状态转换的开始。随着时间推移，即可定量估算SIS的可靠性。

马尔可夫图主要包含2个元素：表示系统状态的圆圈和表示不同状态之间的转换弧线。见图G.1。



图G.1 简单模型

状态1，是在正常运行的原件状态。状态2是故障但可以修复的原件的状态。正常运行状态可以失效，转换为状态2；故障但可以维修的状态可以经过维修，转换为正常状态。

G.2 建模原理

当进行马尔可夫分析时，需要构造一个马尔可夫图，也称为状态转移图。马尔可夫图表示系统的状态及其在不同状态之间的转换。

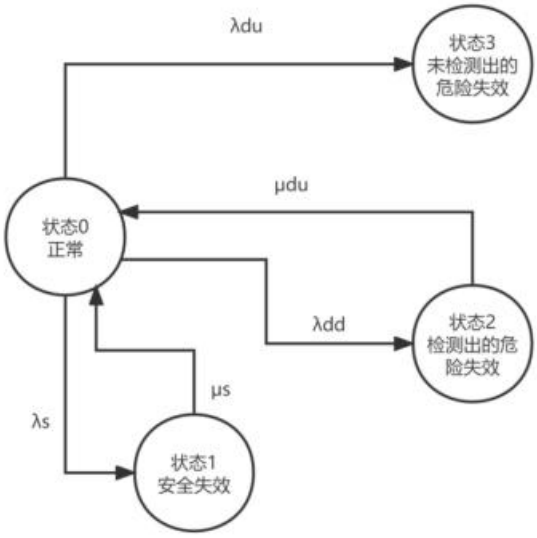
为了便于读者理解，本附录以1oo1架构的马尔可夫建模进行举例，说明马尔可夫建模的详细过程。本附录的目的是讲解马尔可夫建模的方法原理，并不针对具体的1oo1D、1oo2、1oo3、2oo3等其他表决情况建模分析。

马尔可夫建模过程需要详细了解各种故障率和修复率，以及使用一个数学模型，如状态转移矩阵来计算处于每个状态的概率。

状态转移矩阵是马尔可夫模型的核心部分，它是系统在一个定义的时间间隔Δt内从一种状态过渡到另一种状态的概率矩阵。时间间隔的长度影响计算的精度，间隔越小，精度越高。转移概率矩阵包含了关于系统转移的所有信息。我们使用图G.2开发一个示例矩阵来说明该方法。

在实际应用中，分析人员可以只关注模型的构建，而不是基础的数学运算。不过，至少应该理解本附录所介绍的方法原理。关于马尔可夫方法的更详细的讨论，读者可以参考ISO TR 12489—2013。

故障安全和故障危险模式的马尔可夫模型如下：



图G.2 故障安全和故障危险的马尔可夫图

状态0是正常无故障状态，状态1是安全检测的失效状态，状态2是可检测出危险的失效状态，状态3是未检测出危险的失效状态。其中各个状态的转换关系如上图G.2所示。假设未检测出危险的失效状态不能在线维修修复。

G.2.1 建模过程

建模过程主要分为三个部分：

1. 定义系统可能出现的状态，系统状态在马尔可夫图中用圆表示。
   状态0：安全状态
   状态1：安全失效
   状态2：检测出危险失效
   状态3：未检测出危险失效
2. 列出系统状态之间可能发生转换的情况，转换在马尔可夫图中用有向弧线表示。
   状态0-->状态1 发生安全失效
   状态0-->状态2 发生检测出的危险失效
   状态0-->状态3 发生未检测出的危险失效
   状态1-->状态0 安全失效被修复
   状态2-->状态0 检测出的危险失效被修复
3. 计算状态之间转换的概率。
   状态0-->状态1 安全失效率 λs
   状态0-->状态2 检测出的危险失效率 λdd
   状态0-->状态3 未检测出的危险失效 λdu
   状态1-->状态0 安全失效修复率 μs
   状态2-->状态0 检测出的危险失效修复率 μdd

G.2.2 转移矩阵

对于具有N个系统状态的马尔可夫图，转移概率矩阵是一个NxN个覆盖所有可能的转移矩阵。例如，图G.2有4种状态，所以转移概率矩阵是一个4x4的矩阵。表G.1矩阵是通过使用模型中定义的圆弧(转换概率)来填充的。

表G.1 安全失效/危险失效马尔可夫模型的转移概率矩阵

	转移状态			
初始状态	0	1	2	3
0	1-λs-λdd-λdu	λs	λdd	λdu
1	mμs	1-μs	0	0
2	mμdd	0	1-μdd	0
3	0	0	0	1

已知 λs= 0.001, μs= 0.04, λdd=0.06, μdd=0.125, λdu=0.03，带入转移矩阵得到量化的转移概率矩阵。见表G.2。

表G.2 安全失效/危险失效马尔可夫模型的量化转移概率矩阵

转移概率			
0.909	0.001	0.06	0.03
0.04	0.96	0	0
0.125	0	0.875	0
0	0	0	1

G.2.3 矩阵运算

给定时间t时刻的概率计算公式用一个向量微分方程G-1来表示：

$$\vec{P}(t) = e^{t[M]}\vec{P}(0) \qquad (G\text{-}1)$$

[M]为包含转移率的马尔可夫矩阵，$\vec{P}(0)$为初始条件向量(通常为一个列向量，完好状态为1，其他状态为0),如[1,0,0,0]。

尽管矩阵指数的属性与普通指数不完全相同，也可以得出如下方程 G-2：

$$\vec{P}(t) = e^{(t-t_1)[M]}e^{t_1[M]}\vec{P}(0) = e^{(t-t_1)[M]}\vec{P}(t_1) \qquad (G\text{-}2)$$

这描述了马尔可夫过程的基本属性：给定t_1时刻的状态概率概括了所有过去演变的相关信息，并足以用来计算从t_1时刻起系统的未来是如何演变的。

通过方程G-2 可以得出前 10 个时刻的马尔可夫模型概率，见表G.3。

表G.3 安全失效/危险失效马尔可夫模型的部分时间概率

时刻	状态 0	状态 1	状态 2	状态 3
0	1.000	0.0000	0.0000	0.0000
1	0.9090	0.0010	0.0600	0.0300
2	0.8338	0.0019	0.1070	0.0573
3	0.7714	0.0026	0.1437	0.0823

时刻	状态 0	状态 1	状态 2	状态 3
4	0.7193	0.0033	0.1720	0.1054
5	0.6754	0.0039	0.1937	0.1270
6	0.6383	0.0044	0.2100	0.1473
7	0.6067	0.0049	0.2220	0.1664
8	0.5794	0.0053	0.2307	0.1846
9	0.5557	0.0056	0.2366	0.2020

案例中的马尔可夫模型中处于危险失效的状态是状态 2 和状态 3，所以PFD是为状态 2 和状态 3 的概率之和，而PFDavg是所有PFD的平均值。

PFDavg可通过平均累计时间(MCT)进行计算,参考公式G-3 和G-4。

$$\vec{MCT}(T)=\int_0^T \vec{P}(t)dt \qquad \text{(G-3)}$$

对于$\vec{P}(t)$，使用已有的成熟算法进行[0,T]间的积分运算，最后可得：

$$PFD\ \mathbf{avg}\ (T)=\frac{1}{T}\sum_{k=1}^{n} q_k MCT_k(T) \qquad \text{(G-4)}$$

其中，如果系统在状态k时为不可用，则q_k=1，在其他情况下q_k=0。

G.3 简化公式

马尔可夫方法有一定的优缺点。主要优点是其建模的灵活性。例如，在一个马尔可夫模型中，可以对不同组件的不同失效模式、不同组件或不同的修复率（即在线、离线、周期性、不完善的测试和修复、诊断能力、与时间相关的失效序列和常见失效原因）进行建模。一旦建立了马尔可夫模型，所有的信息都可用来计算按需失效的PFDavg或STR。

其主要缺点是其计算和建模的复杂性。马尔可夫模型的构建被用户和实践者视为最大的缺点。目前这些模型通常都是手工构建的。对于相对复杂的SIS，马尔可夫模型的构建变得耗时和繁琐。当系统进一步增长时，马尔可夫模型变得难以管理。如果不进行大量的近似，采用人工进行马尔可夫方法建模和计算就会变得非常困难。因此，可采用简化公式来计算，见表G.4。

表G.4 考虑到CCF、诊断和MTTR的不同表决的“平均后”PFDavg公式

	“平均后”PFDavg公式
1 取 1	$\frac{1-DC\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR$
2 取 1	$\left[\frac{1}{3}\left[(1-DC)\times(1-\beta)\times\lambda^D\times TI\right]^2+(1-DC)DC\times\left[(1-\beta)\times\lambda^D\right]^2\times TI\left(\frac{DI}{2}+MTTR\right)\right]+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$

	“平均后”PFDavg公式
3 取 1	$\left[\frac{1}{4}\left[(1-DC)\times(1-\beta)\times\lambda^{D}\times TI\right]^{3}+(1-DC)^{2}DC\times\left[(1-\beta)\times\lambda^{D}\right]^{3}\times TI^{2}\left(\frac{DI}{2}+MTTR\right)\right]+\left[\frac{(1-DC)\times\beta\times\lambda^{D}\times TI}{2}+\frac{DC\times\beta\times\lambda^{D}\times DI}{2}+\beta\times\lambda^{D}\times MTTR\right]$
2 取 2	$2\times\left[\frac{(1-DC)\times\lambda^{D}\times TI}{2}+\frac{DC\times\lambda^{D}\times DI}{2}+\lambda^{D}\times MTTR\right]$
3 取 2	$\left[\left[(1-DC)\times(1-\beta)\times\lambda^{D}\times TI\right]^{2}+3\times(1-DC)DC\times\left[(1-\beta)\times\lambda^{D}\right]^{2}\times TI\left(\frac{DI}{2}+MTTR\right)\right]+\left[\frac{(1-DC)\times\beta\times\lambda^{D}\times TI}{2}+\frac{DC\times\beta\times\lambda^{D}\times DI}{2}+\beta\times\lambda^{D}\times MTTR\right]$
3 取 3	$3\times\left[\frac{(1-DC)\times\lambda^{D}\times TI}{2}+\frac{DC\times\lambda^{D}\times DI}{2}+\lambda^{D}\times MTTR\right]$

对于 1oo2、1oo3 和 2oo3 表决，公式的第一部分用于IF，第二部分用于CCF。在公式的第一部分中，两个或两个以上DD故障的独立失效被认为可以忽略不计。第一部分的第二项表示由于修复而不可用，对于较短的平均修复时间通常可以忽略不计。

附录H
（资料性）
计算示例和方法比较

H.1 介绍

计算例子包括：H.2 计算PFDavg、H.3 计算STR。

H.2 计算PFDavg

本例说明3种SIF计算方法，并比较结果。

a) 故障树模型图形软件法（图形法）：见计算图。来自ISA TR84.00-02—2022 附录H。

b) 马尔可夫法：仅罗列ISA标准中的结果，参与比较。

c) 故障树模型公式软件法（公式法）：见计算表。计算表中使用的公式见附录E、F。

计算对象和输入数据相同。参与计算的共用设备的参数见表H.1。

表H.1 共用输入数据

表中的数据（A）						图中的数据及反算（B）				反算结果用于使用（C）			
代码	类型	λD /年	λS /年	MTTR 小时	CCF	Tau	Q	Q/Tau×2 DU部分	DD部分	λDU FIT	λDD FIT	λSU FIT	λSD FIT
PT	Pressure transmitter	1.31 E-3	1.31 E-3	72	2%	5	3.28 E-3	1.31 E-3	-2.00 E-6	150	0	150	0
TA	Trip Amplifiter (Analog Relay)	3.50 E-4	3.50 E-4	72	1%	5	8.77 E-4	3.51 E-4	-8.00 E-7	40	0	40	0
SV	Solenoid Valve (De-energrize to trip)	1.67 E-2	3.33 E-2	72	1%	5	4.07 E-2	1.63 E-2	4.20 E-4	1858	48	3801	0
BV	Block Valve (Fail to Close)	2.72 E-2	4.38 E-3	72	1%	5	6.52 E-2	2.61 E-2	1.12 E-3	2977	128	500	0
注1：参见ISA TR84.00-02—2022 附录H 表H.1、图H.2。 注2：ISA表H.1仅列出部分的输入数据，即本表A部分。 注3：本表补足了全部输入数据。即：从ISA图H.2通过反算（本表B部分），列出其他的输入数据（本表C部分）。													

例子清单、简要说明、结果见表H.2，3种方法的计算结果基本相同。

表H.2 汇总比较

例子和配置			TI = 1 年			TI = 5 年		
编号	传感器	最终元件	图形法	马尔可夫法	公式法	图形法	马尔可夫法	公式法
H.2.1	1取1	1取1	2.28 E-2	2.24 E-2	2.20 E-2	1.07 E-1	1.06 E-1	1.10 E-1
H.2.2	2取1	1取1	2.20 E-2	2.17 E-2	2.12 E-2	1.03 E-1	1.02 E-1	1.06 E-1
H.2.3	2取2	1取1 2取2	3.19 E-2	3.14 E-2	3.10 E-2	1.47 E-1	1.44 E-1	1.55 E-1
H.2.4	3取2	1取1 2取2	3.03 E-2	2.98 E-2	2.93 E-2	1.40 E-1	1.37 E-1	1.47 E-1
H.2.5	1取1	2取1	1.55 E-3	1.66 E-3	1.49 E-3	1.58 E-2	1.87 E-2	1.64 E-2
H.2.6	2取2	2取1 2取2	2.82 E-3	未提供	2.81 E-3	2.86 E-2	未提供	3.13 E-2
H.2.7	2取1	2取1	7.78 E-4	7.18 E-4	6.78 E-4	1.18 E-2	1.47 E-2	1.24 E-2
H.2.8	3取2	2取1 2取2	1.14 E-3	未提供	1.17 E-3	2.07 E-2	未提供	2.31 E-2
注：最终元件的"1取1 2取2"配置指：整体阀门是1取1配置，阀门的电磁阀是2取2配置。								

每个例子都包括以下。为简洁，每个例子不再重复说明。

a) 1个工艺简图：图示计算对象；

b) 1个计算图：故障树图形法的计算过程，仅编入5年TI的情况；

c) 1个计算表：故障树公式法的计算过程，仅编入5年TI的情况。

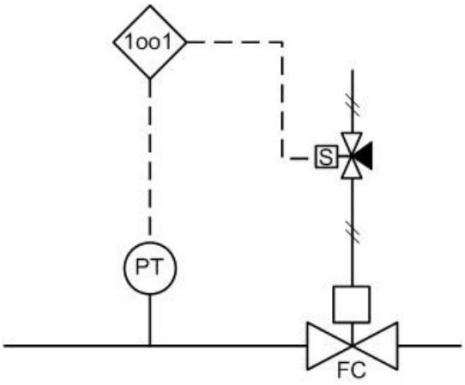
计算说明如下：

a) 为了简化，仅考虑 λ_{DU}。

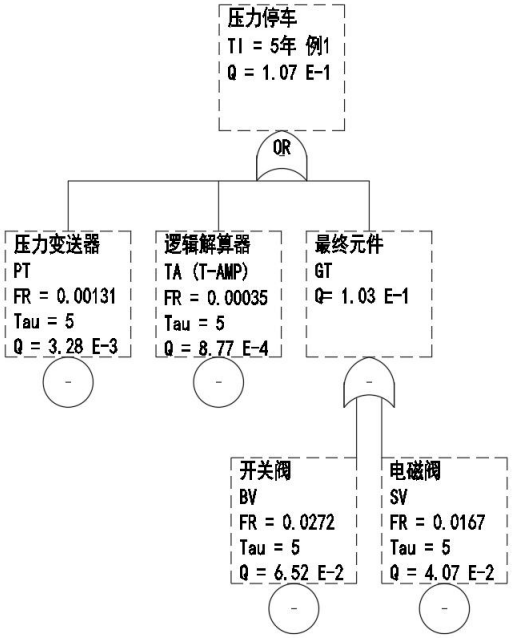
b) 例子中，为方便比较，在CCF部分，没有剔除IF。例子H.2.5的计算表，典型标注了这些内容。即：2取2开关阀的失效，应分为CCF、IF，分别分析；但本例子针对全部（CCF+IF）、IF，分别分析。实际计算中CCF部分需剔除IF。

注：故障树计算图摘录自ISA标准，因原始文件不清晰，所以有些数据是空缺的。但不影响计算结果。故障数中的代码无专门释意，但不影响可读。

H.2.1　例子：工艺简图见图H.1，计算图见图H.2，计算表见表H.3。



图H.1 工艺简图



图H.2 计算图

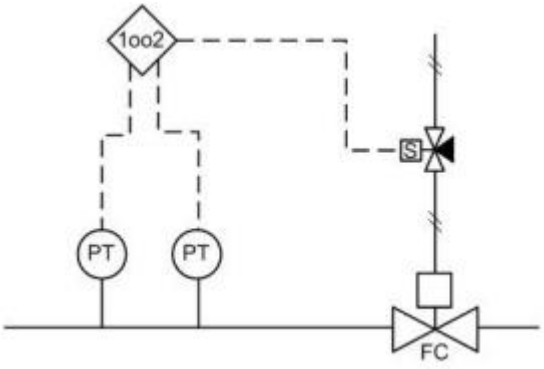
表H.3 计算表

随机失效　　1.10 E-1 总计

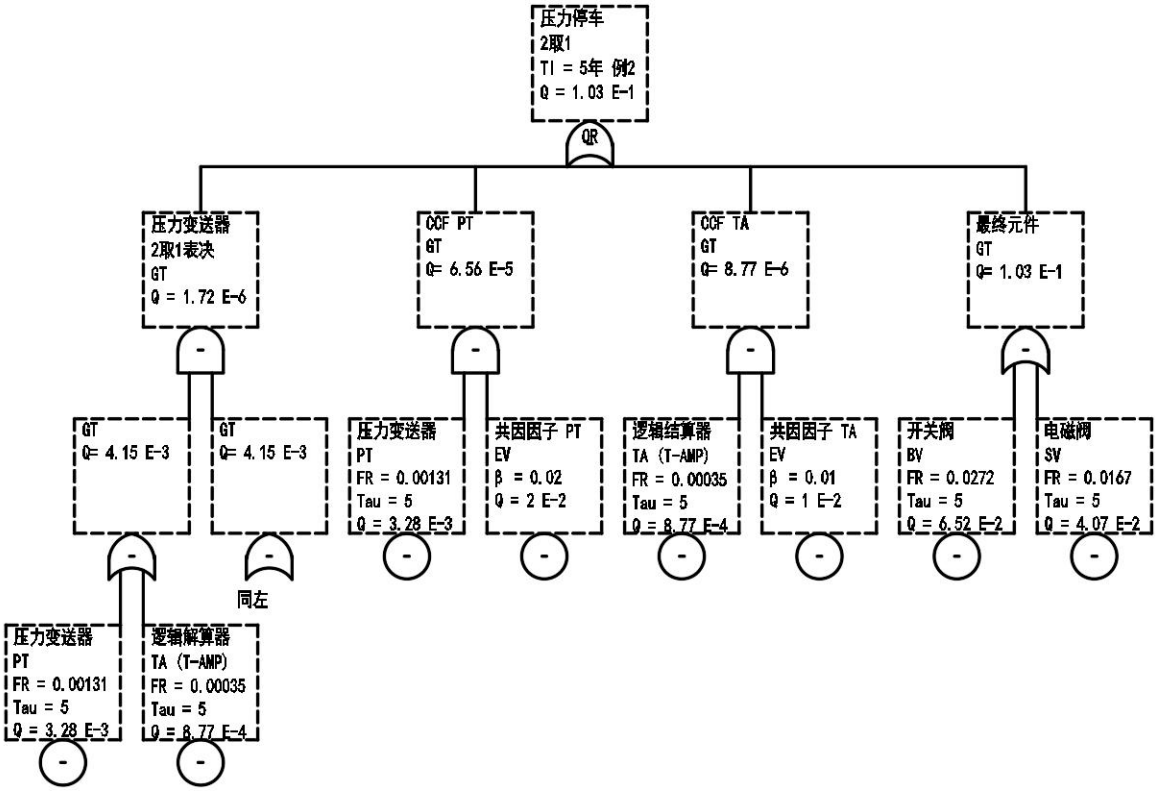
子系统	各部分分计配置 PFD	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	3.3 E-3 等效	测量	3.3 E-3	1取1			PT-1	150	串联	PT	150
逻辑解算器	8.8 E-4 等效	器件	8.8 E-4	1取1			TA-1	40	串联	TA	40
最终元件	1.1 E-1 等效	阀门	1.1 E-1	1取1			V-1	4836	串联	SV	1858

H.2.2　例子：工艺简图见图H.3，计算图见图H.4，计算表见表H.4。

本例的计算图、计算表中，PT和TA都属于传感器部分。按通常习惯，PT属于传感器；TA属于逻辑解算器。按计算原理，归属关系不影响计算结果。



图H.3 工艺简图



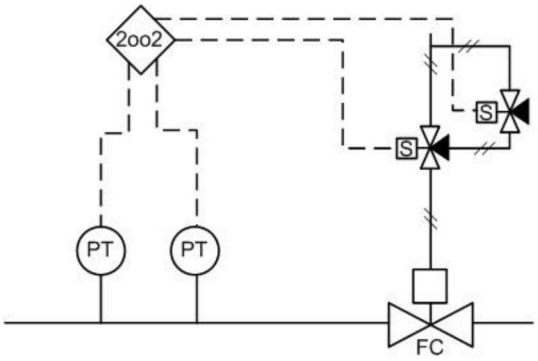
图H.4 计算图

表H.4 计算表

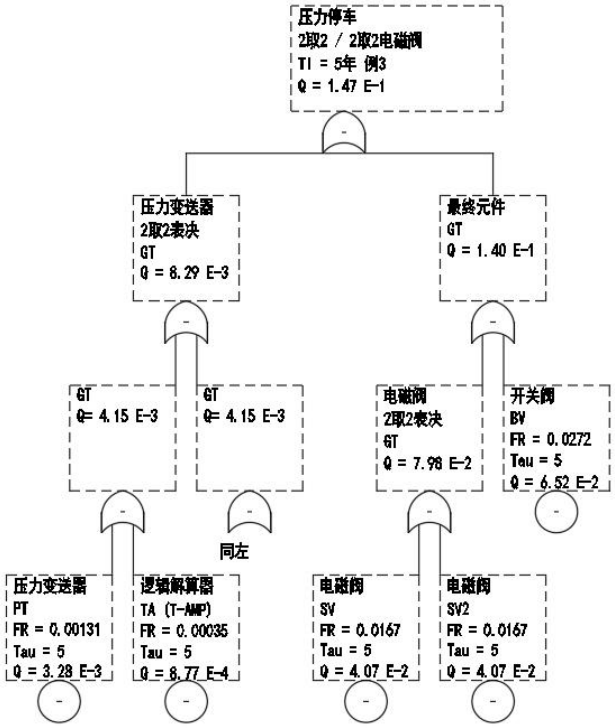
随机失效　　1.06 E-1 总计

子系统	各部分分计配置 PFD		部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	1.0 E-4	等效	测量	1.0 E-4	2取1	2%	72	PT-1	189	串联	PT	150
				注：CCF中的IF							TA	40
								PT-2	189	复用		
最终元件	1.1 E-1	等效	阀门	1.1 E-1	1取1			V-1	4836	串联	SV	1858
											BV	2977

H.2.3　例子：工艺简图见图H.5，计算图见图H.6，计算表见表H.5。



图H.5 工艺简图



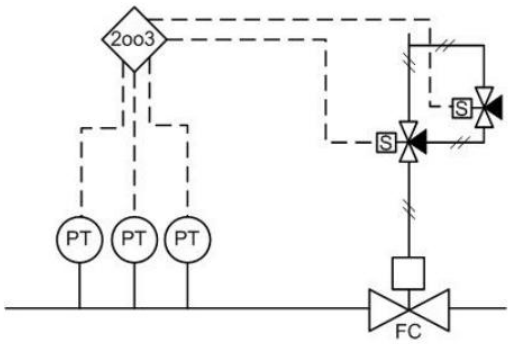
图H.6 计算图

表H.5 计算表

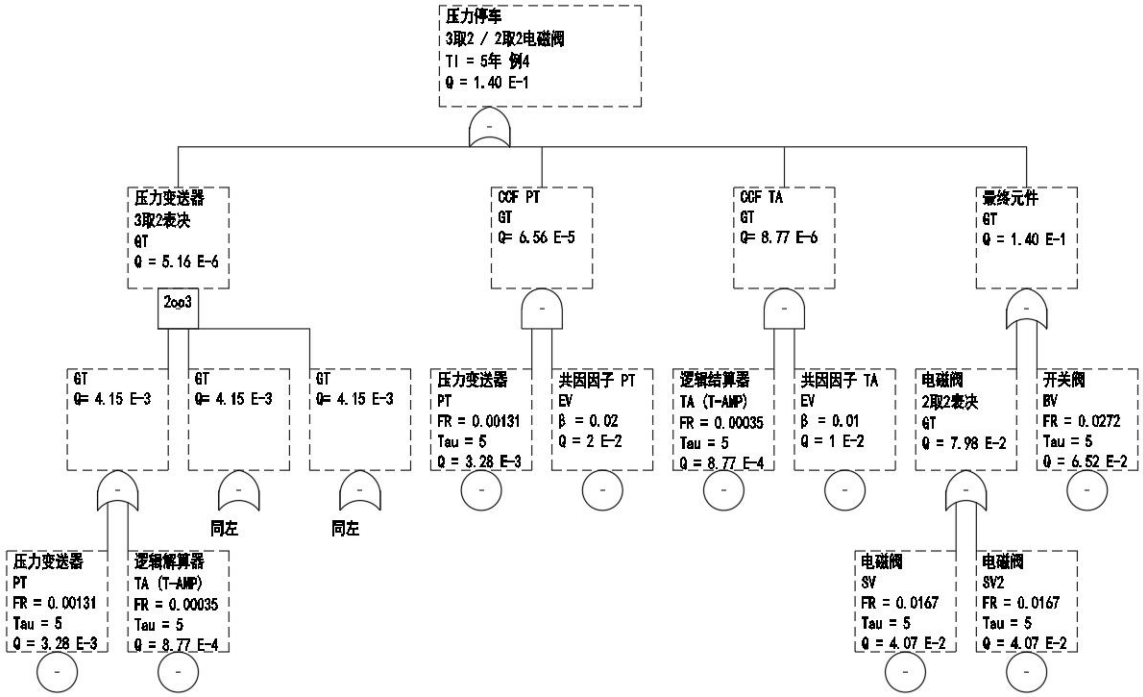
随机失效　　1.55 E-1 总计

子系统	各部分分计PFD	配置	部分	PFD	配置	β	MTTR小时	仪表位号	λDU	配置	组件名称	λDU
传感器	8.3 E-3	等效	测量	8.3 E-3	2取2		72	PT-1	190	串联	PT	150
											TA	40
								PT-2	189	复用		
最终元件	1.5 E-1	等效	阀门	1.5 E-1	1取1			V-1	6694	串联	SV	3717
											BV	2977
			电磁阀等效 并联：可靠性低，可用性高；等效计算后，作为组合使用等效λ。									
				8.1 E-2	2取2		72	SV1	1858			1858
				3717				SV2	1858			1858

H.2.4　例子：工艺简图见图H.7，计算图见图H.8，计算表见表H.6。



图H.7 工艺简图



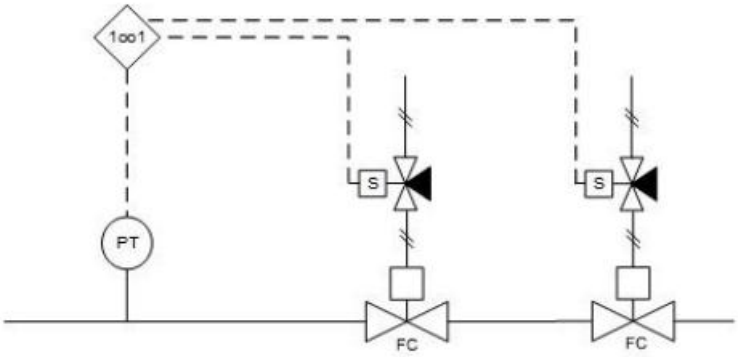
图H.8 计算图

表H.6 计算表

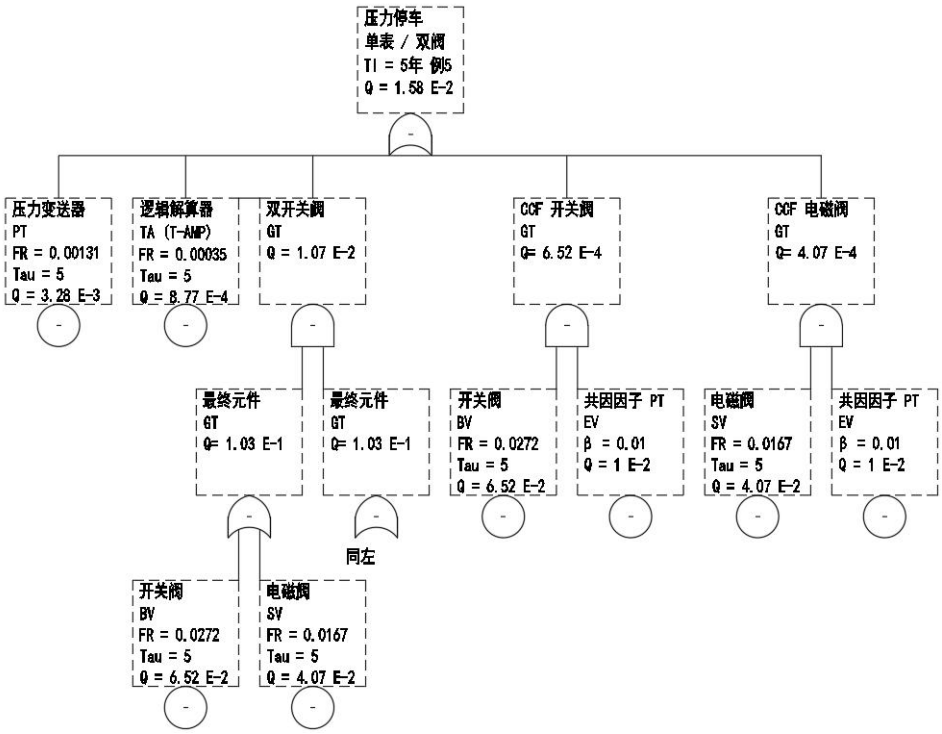
随机失效　　1.50 E-1 总计

子系统	各部分分计 PFD	配置	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	1.2 E-4	等效	测量	1.2 E-4	3取2	2%	72	PT-1	150	串联	PT	150
								PT-2	189	复用		
								PT-3	189	复用		
逻辑解算器	1.1 E-5	等效	器件	1.1 E-5	3取2	1%	72	TA-1	40	串联	TA	40
								TA-2	40	复用		
								TA-2	40	复用		
最终元件	1.5 E-1	等效	阀门	1.5 E-1	1取1			V-1	6822	串联	SV	3717
											BV	3105
			电磁阀并联 等效：可靠性低，可用性高；等效计算后，作为组合使用等效λ。									
				8.1 E-2	2取2	1%	72	SV1	1858			1858
				3717				SV2	1858			1858

H.2.5　例子：工艺简图见图H.9，计算图见图H.10，计算表见表H.7。



图H.9 工艺简图



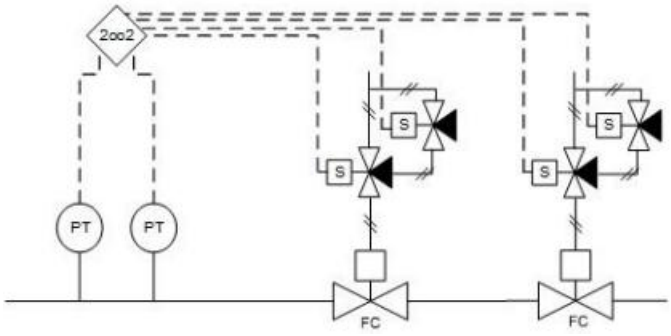
图H.10 计算图

表H.7 计算表

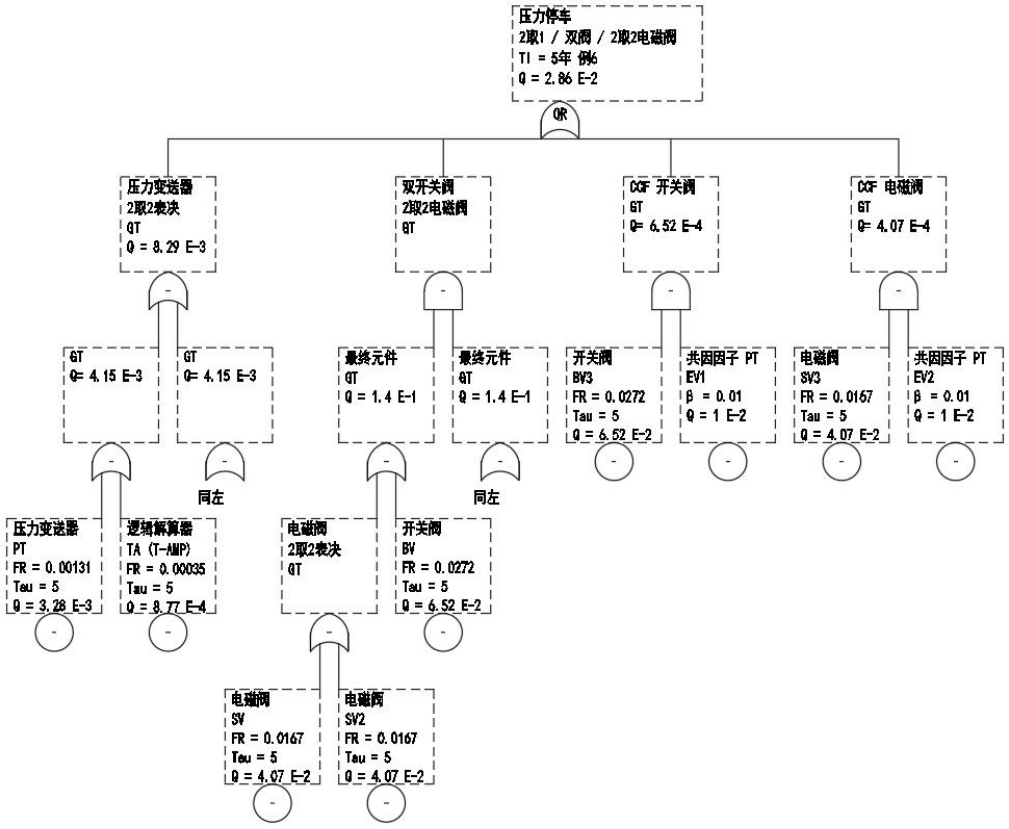
随机失效　　1.64 E-2 总计

子系统	各部分分计 PFD	配置	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	3.3 E-3	等效	测量	3.3 E-3	1取1			PT-1	150	串联	PT	150
逻辑解算器	8.8 E-4	等效	器件	8.8 E-4 注A	1取1			TA-1	40	串联	TA	40
最终元件	1.2 E-2	等效	阀门	1.23 E-2	2取1	1%	72	V-1	4836	串联	SV	1858
			注B	1.12 E-2							BV	2977
			注C	1.06 E-3								
			注D	1.21 E-2								
			注A：本例计算的值，方便与ISA例子比较。					V-2	4836	复用		
			注B：A中CFF部分，此部分已特殊处理。未剔除IF（1%）。									
			注C：A中IF部分。									
			注D：应计算的值，与实际应用一致。									
			注：CCF中的IF									

H.2.6　例子：工艺简图见图H.11，计算图见图H.12，计算表见表H.8。



图H.11　工艺简图



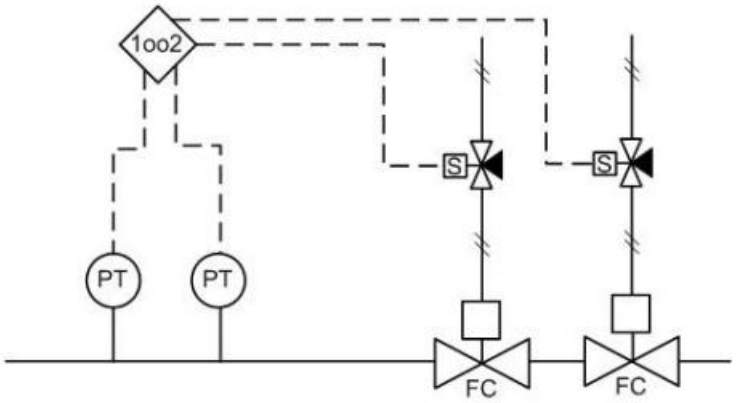
图H.12　计算图

表H.8　计算表

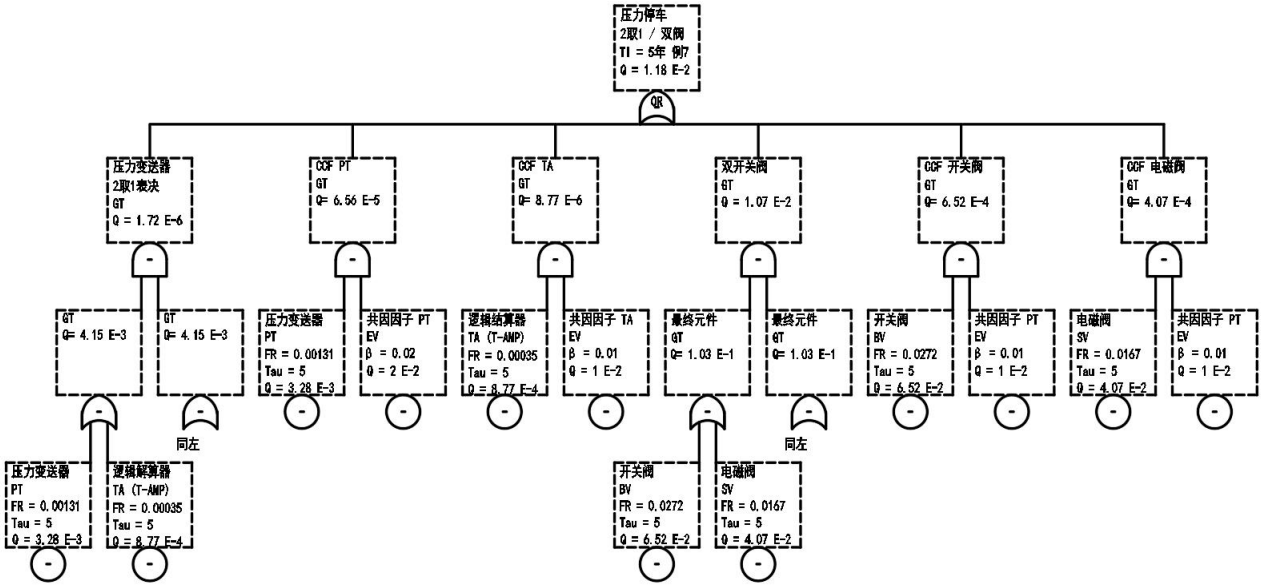
随机失效　　3.13 E-2 总计

子系统	各部分分计 PFD	配置	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	8.3 E-3	等效	测量	8.3 E-3	2取2		72	PT-1	189	串联	PT	150
											TA	40
								PT-2	189	复用		
最终元件	2.3 E-2	等效	阀门	2.3 E-2	2取1	1%	72	V-1	6694	串联	SV	3717
				注：CCF中的IF							BV	2977
								V-2	6694	复用		
			电磁阀并联 等效：可靠性低，可用性高；等效计算后，作为组合使用等效λ。									
				8.1 E-2	2取2		72	SV1	1858			1858
				3717				SV2	1858			1858

H.2.7　例子：工艺简图见图H.13，计算图见图H.14，计算表见表H.9。



图H.13 工艺简图



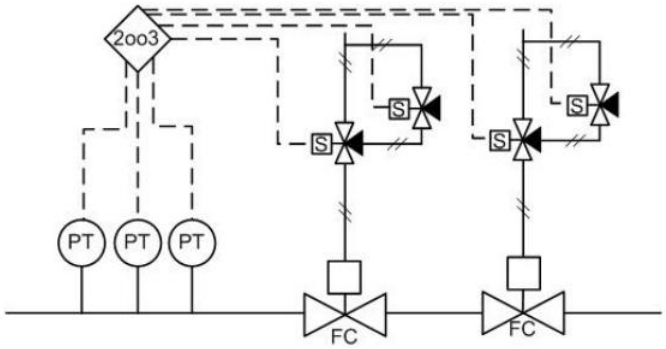
图H.14 计算图

表H.9 计算表

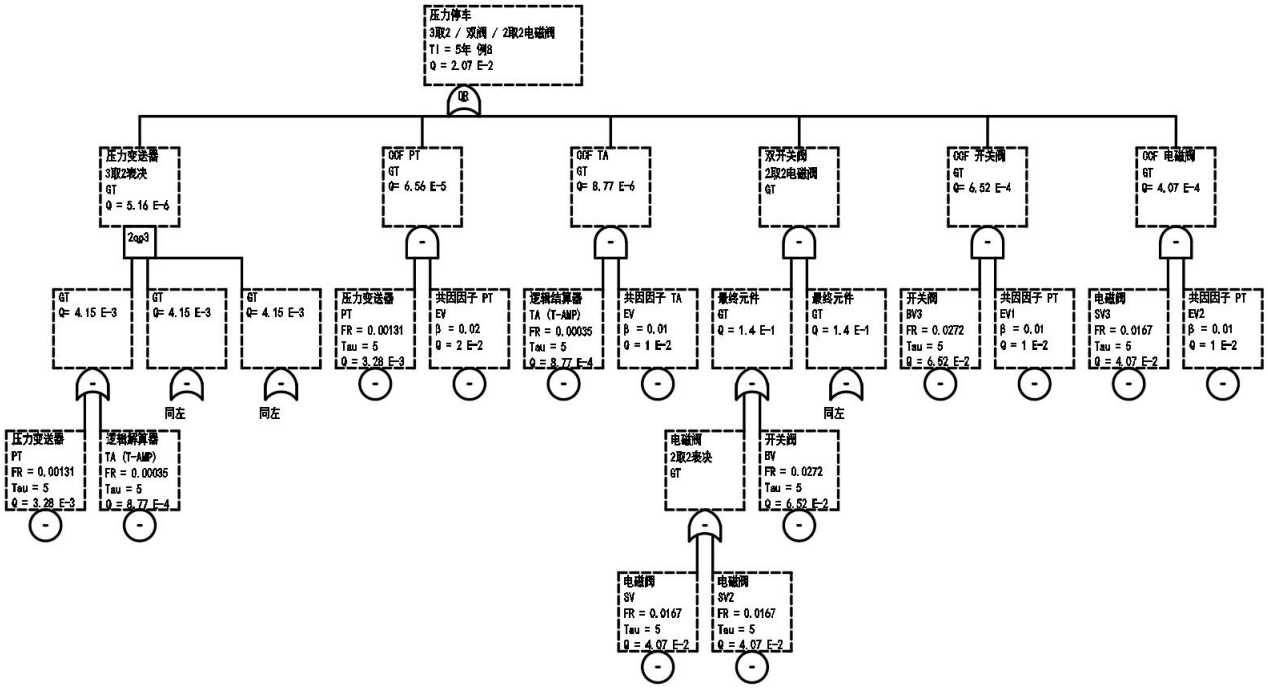
随机失效　　1.24 E-2 总计

子系统	各部分分计PFD	配置	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	1.0 E-4	等效	测量	1.0 E-4	2取1	2%	72	PT-1	189	串联	PT	150
				注：CCF中的IF		1%					TA	40
								PT-2	189	复用		
最终元件	1.2 E-2	等效	阀门	1.2 E-2	2取1	1%	72	V-1	4836	串联	SV	1858
				注：CCF中的IF							BV	2977
								V-2	4836	复用		

H.2.8　例子：工艺简图见图H.15，计算图见图H.16，计算表见表H.10。



图H.15 工艺简图



图H.16 计算图

表H.10 计算表

随机失效　　1.17 E-3 总计

子系统	各部分分计 PFD	配置	部分	PFD	配置	β	MTTR 小时	仪表位号	λDU	配置	组件名称	λDU
传感器	1.9 E-5	等效	测量	1.9 E-5 注：CCF中的IF	3取2	2%	72	PT-1	189	串联	PT	150
											TA	40
								PT-2	189	复用		
								PT-3	189	复用		
最终元件	1.2 E-3	等效	阀门	1.2 E-3 注：CCF中的IF	2取1	1%	72	V-1	6694	串联	SV	3717
											BV	2977
								V-2	6694	复用		
电磁阀并联 等效：可靠性低，可用性高；等效计算后，作为组合使用等效λ。												
				1.6 E-2	2取2	1%	72	SV1	1858			1858
				3717				SV2	1858			1858

H.3 计算STR 例子

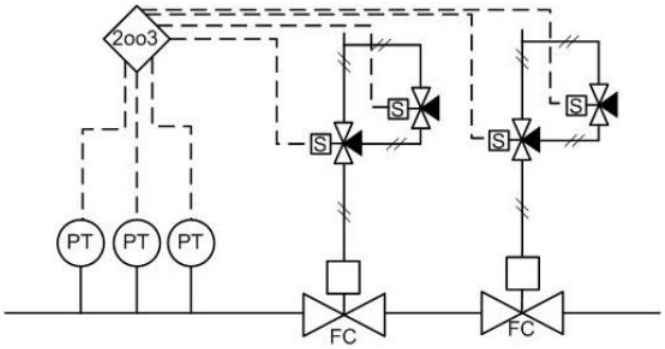
本例说明3种SIF计算方法，并比较结果。

a) 分析故障过程，并计算的方法（过程法）：见ISA TR84.00-02—2022附录H。

b) 马尔可夫法：仅罗列ISA标准中的结果，参与比较。

c) 故障树建模公式软件法（公式法）：计算表，见表H.12。

计算对象和输入数据相同，见图H.17、表H.11。



图H.17 工艺简图

表H.11 输入数据

表中的数据					反算结果用于使用			
代码	类型	λSP /年	MTTR 小时	CCF	λDU FIT	λDD FIT	λSU FIT	λSD FIT
PT	Pressure transmitter	1.31 E-3	72	2%			150	
TA	Trip Amplifiter (Analog Relay)	3.50 E-3	72	1%			400	
SV	Solenoid Valve (De-energrize to trip	3.33 E-2	72	1%			3801	
BV	Block Valve (Fail to Close)	4.38 E-3	72	1%			500	
注1：TI = 5年。在本例中参与计算。								

表H.12 计算表

随机失效 2.3 E-6 总计
2.00 E-2 /年

子系统 STR		配置	部分	STR	STR-TI 选择	配置	β	MTTR 小时	仪表位号	λSP	配置	组件名称	λSP
传感器 1.1 E-6	1.3 E-10	等效	测量	1.3 E-10	N	3取2	2%	72	PT-1	549	串联	PT	150
				本数未拆分IF/CFF。占比小，不影响结果。								TA	400
									PT-2	549	复用		
									PT-3	549	复用		
最终元件 2.0 E-2	2.3 E-6	等效	阀门	2.3 E-6		2取1	1%	72	V-1	1135	串联	SV	635
												BV	500
									V-2	1151	复用		
			电磁阀并联 等效：可靠性低，可用性高；等效计算后，作为组合使用等效λ。										
				6.4 E-7	Y	2取2	1%	72	SV1	3801			3801
				635					SV2	3801			3801

3种方法的结果一致，见表H.13。

表H.13 结果比较（单位：/年）

过程法	马尔可夫法	公式法
2.00 E-2	2.04 E-2	2.00 E-2

附录I
（资料性）
失效模式与影响分析FMEA示例

电子变送器的FMEA的示例见表I.1、图I.1。

每一个失效产生一个错误信号，分为降级（部分）失效和完全失效。依据是规格书和测试不合格的标准。

这些失效进一步分级如下。依据是对设备使用的影响。

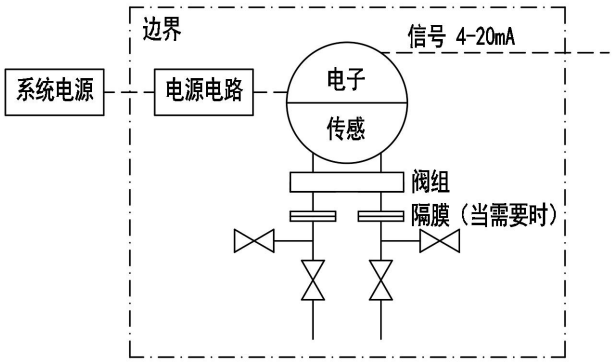
如果工艺参数高时，处于停车状态，则变送器错误输出高是安全失效。

如果工艺参数低时，处于停车状态，则变送器错误输出高是危险失效。

表I.1 FMEA示例

失效模式	失效分级	失效原因	失效机理
完全失效			
信号输出>100%	根据应用（注 1）	电子故障	腐蚀、老化、热应力
信号输出冻结	危险	隔离阀关闭	人为错误
		导压管堵塞	固体存积、液体冻结
		设为测试模式	人为错误
		电子故障	腐蚀、老化、热应力
信号输出<0%	根据应用（注 2）	电子故障	腐蚀、老化、热应力
部分失效			
信号输出高	根据应用（注 1）	电子故障	腐蚀、老化、热应力
		调整范围之外	人为错误
		传感器损坏	水锤
		导压管内物料堆积	错误安装、工艺异常
信号输出低	根据应用（注 2）	电子故障	腐蚀、老化、热应力
		调整范围之外	人为错误
		传感器损坏	水锤
信号输出反应慢	根据总安全时间（注 3）	导压管部分堵塞	固体部分存积、液体部分冻结
		导压管卷曲	机械损伤
		填充液泄露	机械损伤、材料腐蚀
		填充液泄露	震动、腐蚀、机械损伤
		电子故障	腐蚀、老化、热应力
信号输出反应快	根据应用	电子故障	腐蚀、老化、热应力
信号输出无规律	危险	电子故障	腐蚀、老化、热应力
公用工程影响			
电源高	早期条件，制造更大的应力，最终带来危险或安全失效。	电子故障	错误安装、错误设计
电源低	危险	电子故障	错误安装、错误设计

失效模式	失效分级	失效原因	失效机理
无电源	安全（非励磁停车时） 危险（励磁停车时）	电子故障	错误安装、错误设计
电源突变	安全或危险	电容故障	电容耗尽
		EMI / RFI	错误安装、错误设计
注 1：工艺参数高停车时，是安全失效；工艺参数低停车时，是危险失效。 注 2：工艺参数低停车时，是安全失效；工艺参数高停车时，是危险失效。 注 3：超过总安全时间的部分，为危险失效。			



图I.1 边界图