ICS 13.200
CCS C 68

团　　体　　标　　准

T/CCSAS 045—2023

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)

2023-11-27 发布　　2023-11-27 实施

中国化学品安全协会　发布
中国标准出版社　出版

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、中石油华东设计院有限公司、中国化学赛鼎宁波工程有限公司、中国寰球工程有限公司、万华化学集团股份有限公司、浙江石油化工有限公司。

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、林洪俊、张志、王雪梅、李才华、陆兴旺。

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,提供了验证方法、公式、示例、数据等内容,给出了失效率、结构约束、系统性能力等验证的程序、内容等说明。

本文件适用于石油化工和化工装置的SIL验证。

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 20438.2—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

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

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

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

3 术语和定义

GB/T 20438.4—2017和GB/T 21109.1—2022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:SIF设计用来达到一个要求的SIL,SIL由其他参与降低相同风险的保护层决定。

[来源:GB/T 21109.1—2022,3.2.66]

3.2

安全完整性等级 safety integrity level;SIL

为规定SIS应达到的安全完整性要求而分配给SIF的离散等级(4个等级中的一个)。

注1:SIL等级越高,期望的PFD_{avg}、PFH越低。

注2:目标失效量和SIL间的关系见GB/T 21109.1—2022的表4和表5。

注3:SIL4是安全完整性的最高等级,SIL1是最低等级。

注4:此定义和GB/T 20438.4—2017中的定义有差别,从而反映过程领域术语中的差异。

[来源:GB/T 21109.1—2022,3.2.69,有修改]

3.3

验证 verification

通过检查和客观证据证实要求已满足。

注：本文件的范围是 SIL 验证，不包括对 SIS 的其他的检查、确认。

[来源：GB/T 21109.1—2022，3.2.87，有修改]

3.4

故障裕度　fault tolerance

出现故障或错误时，功能单元能够继续执行要求的功能或操作的能力。

注 1：硬件故障裕度 HFT=1 表示：当多个组件中的 1 个故障时，单元能工作。

注 2：2oo3 配置的危险故障的 HFT 是 1；1oo3 的是 2。

[来源：GB/T 21109.1—2022，3.2.21，有修改]

3.5

系统性能力　systematic capability；SC

当设备根据安全手册规定的说明进行应用时，设备的系统性安全完整性达到规定 SIL 要求的置信度的度量（表示为 SC 1 到 SC 4），其与特定的安全功能有关。

注 1：系统性能力参照 GB/T 20438.2—2017 和 GB/T 20438.3—2017 中系统性故障的避免和控制要求确定。

注 2：系统性失效机制取决于设备的特性。对于只由硬件组成的设备，只考虑硬件失效机制。对于由硬件和软件组成的设备，则需要考虑硬件和软件失效机制间的相互影响。

注 3：某设备 SC *N* 的系统性能力是指当设备按照安全手册规定的 SC *N* 要求应用时，此设备达到了 SC *N* 的系统性安全完整性。

[来源：GB/T 21109.1—2022，3.2.80]

3.6

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

PFD_{avg}

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：PFD 随时间积累而变化，是时间的函数 PFD(t)；PFD_{avg} 是规定时间段内的平均值。

注 2：对于 SIS，需求时，不能响应，即为危险故障。

注 3：也称为要求时的平均危险失效概率（average probability of dangerous failure on demand）。

[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：此处故障指危险故障。

[来源：ISA TR84.00.02—2022，第 7 章，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：$STR=1/MTTF_{SP}$

[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。

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

注 2：本文件中，TI 及其他时间参数参与计算时，单位是小时（h）。

注 3：检验测试间隔也称检测周期。

[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 Δt 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 Δt 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/h)。

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。

[来源：ISA TR84.00.02—2022，附录 B，有修改]

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

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

下列缩略语适用于本文件。

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)

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 restoration)

PFD：要求时的失效概率(probability of failure on demand)

PFD_{avg}：要求时的平均失效概率(average probability of failure on demand)

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

PTC：检验测试覆盖率(proof test coverage)

PVST：部分阀门行程测试(partial valve stroke test)

注 2：也称为 PST 部分行程测试(partial stroke 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：安全要求规范(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，也可按需使用小写，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(dangerous)；
- DD——危险、检测到的(dangerous detected)；
- DU——危险、未检测到的(dangerous undetected)；
- S——安全(safe)；
- 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 验证的外部关系和内部结构见图 1，以及后续条目的说明。示例见附录 A。

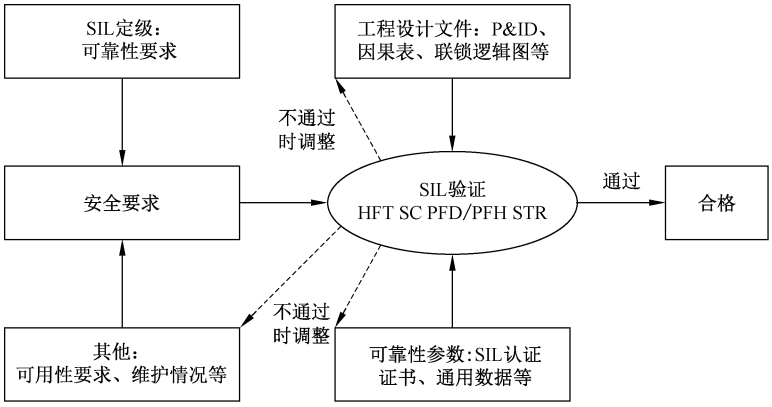


图 1　SIL 验证

5.2　SIL 验证包括设计阶段的初步 SIL 验证、采购后的 SIL 验证、现役装置的 SIL 验证等。

5.3　SIL 验证的输入对象(图 1 中实线箭头)应包括如下,对应的文件见附录 B:

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)　可靠性参数:包括 λ 等参数;

e)　工程设计:包括 P&ID、因果表、逻辑图等文件,用于方便理解验证对象。

5.4　仪表设备的可靠性参数的来源包括: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,可采用拟用产品证书数据或通用数据。

5.5　SIL 验证的工作范围(图 1 中椭圆)应包括:

a)　检查:冗余度(HFT)、系统性能力(SC)、可靠性(PFD_{avg}/PFH)、误停车(STR);

b)　计算:PFD_{avg}/PFH、STR。

注:STR 为可选。

5.6　SIL 验证的检查依据见表 1,计算方法见附录 C。

表 1　SIL 检查表

SIL	PFD_{avg} 注 1、注 2	PFH 注 1、注 2	SC 最小	HFT 最小(结构约束 AC 检查)注 3		
				GB/T 21109.1—2022	GB/T 20438.2—2017 中 A 类	GB/T 20438.2—2017 中 B 类
1	$<10^{-1}$ $\geqslant 10^{-2}$	$<10^{-5}$ $\geqslant 10^{-6}$	1	0	0	0(SFF≥60%时) 1(SFF<60%时)
2	$<10^{-2}$ $\geqslant 10^{-3}$	$<10^{-6}$ $\geqslant 10^{-7}$	2	0(低需求模式时) 1(高需求模式、连续模式时)	0(SFF≥60%时) 1(SFF<60%时)	0(SFF≥90%时) 1(60%≤SFF<90%时) 2(SFF<60%时)
3	$<10^{-3}$ $\geqslant 10^{-4}$	$<10^{-7}$ $\geqslant 10^{-8}$	3	1	0(SFF≥90%时) 1(60%≤SFF<90%时) 2(SFF<60%时)	0(SFF≥99%时) 1(90%≤SFF<90%时) 2(60%≤SFF<90%时)

注 1:当 SIL 定级报告中有具体的 PFD_{avg} 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:操作模式的说明见 C.3.1,A 类/B 类的说明见 5.7,SFF 的说明见 C.2.8。

注 4:STR 的检查依据为用户和项目要求。

5.7 组成 SIF 的组件设备的分类见表 2。

表 2 设备分类表

分类	条件
A 类	要实现安全功能的元器件满足下列全部条件： ● 所有组成元器件的失效模式都被明确定义； ● 故障状况下组件的行为能够完全确定； ● 有充足而可靠的失效数据，可显示出满足所声明的检测到的和未检测到的危险失效的失效率
B 类	不满足以上条件之一

5.8 当计算检查不合格时，可调整输入（图 1 中虚线箭头），并重新计算检查，直至合格。调整对结果的影响见附录 D。

5.9 验证报告的内容应包括：输入整理、计算框图和过程、结果和检查、修改建议、相关产品证书等。

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 总体原则和要求

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。以往使用的术语和定义见 GB/T 21109.1—2022 中的 3.2.51。根据“以往使用”选择设备的要求见 GB/T 21109.1—2022 中的 11.5.3。

6.2 用于逻辑解算器的可编程电子系统应取得功能安全认证。

6.3 SIS 或安全子系统的 TI 的确定宜综合考虑 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 的传感器、最终元件和逻辑解算器可采用不同的 TI。

6.5 当 SIF 的误动作可能造成的损失大于可容忍程度时，可规定可用性要求，并验证 SIF 满足可用性要求，如验证 SIF 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 同一个传感器、逻辑解算器、最终元件可用于不同的 SIF，共用部分应满足所有相关 SIF 的安全技术要求，包括 SIF 要求和 SIL 要求，并应进行验证。

6.8 安全仪表系统应独立于基本过程控制系统，并应独立完成安全仪表功能。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 SIL。

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 可达到的危险失效量。

6.10 SIL 验证计算的输入条件应包括危险失效率（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）、共因因子（β）等。

6.11 在对联锁逻辑确定具体 SIF 时，应区分联锁逻辑中的安全关键设备和非安全关键设备。安全关键设备执行安全仪表功能，非安全关键设备不执行安全仪表功能。安全关键设备是指该设备的动作是将工艺过程转入安全状态必不可少的动作，只有该设备的动作有效执行才能将工艺过程转入安全状态。非安全关键设备是指该设备的动作不是将工艺过程转入安全状态必不可少的动作，该设备的动作失效

不影响通过安全关键设备的动作将工艺过程转入安全状态。

注 1：联锁逻辑不等同于 SIF。联锁逻辑仅表达因果关系；SIF 是对某一场景的保护功能。一个 SIF 明确定义一个保护功能的范围和可靠性要求。一个“联锁逻辑”可能是一个 SIF，也可能包含多个 SIF，反之亦然。

注 2：区分安全关键设备和非安全关键设备、确定 SIF 是 SIL 定级的工作。如果 SIL 验证中发现 SIF 中包括了非安全关键设备，可以提出复核要求并由相关人员确定安全关键设备和非安全关键设备，以及 SIF。

6.12 SIF 中控制阀的阀体、执行机构、电磁阀均应参与 SIL 验算。

6.13 石油化工和化工装置 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对 SIL 验证的影响，检测到故障时的系统行为应符合 GB/T 21109.1—2022 的 11.3 的要求。

6.15 SIF 有变动时（包括仪表设备的型号、软件的版本号、制造商、联锁逻辑、独立和共用、场景等方面的变动），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有关国家标准的要求。

7 过程和执行

7.1 验证程序

7.1.1 SIL 验证节点

SIS 安全生命周期中的“SIS 设计和工程”阶段应开展 SIL 验证，如图 2 所示。“SIS 设计和工程”阶段中的基础工程设计阶段可开展 SIL 预验证，“SIS 设计和工程”阶段中的详细工程设计阶段应开展 SIL 验证。现役装置，SIF 有变动时，按照 6.15 的要求进行 SIL 验证；SIL 验证可按照 6.16 的要求，建立全生命周期的动态机制。

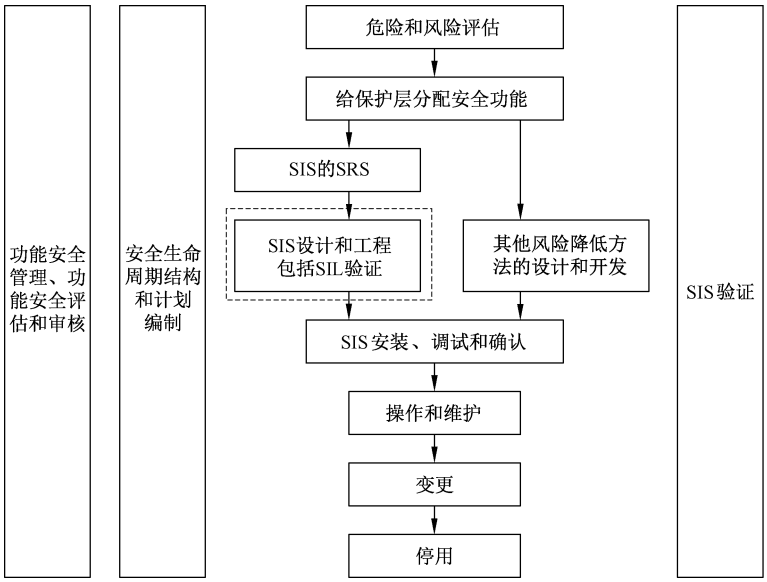


图 2 SIS 安全生命周期框图

7.1.2 SIL 验证程序

典型的 SIL 验证流程如图 3 所示。

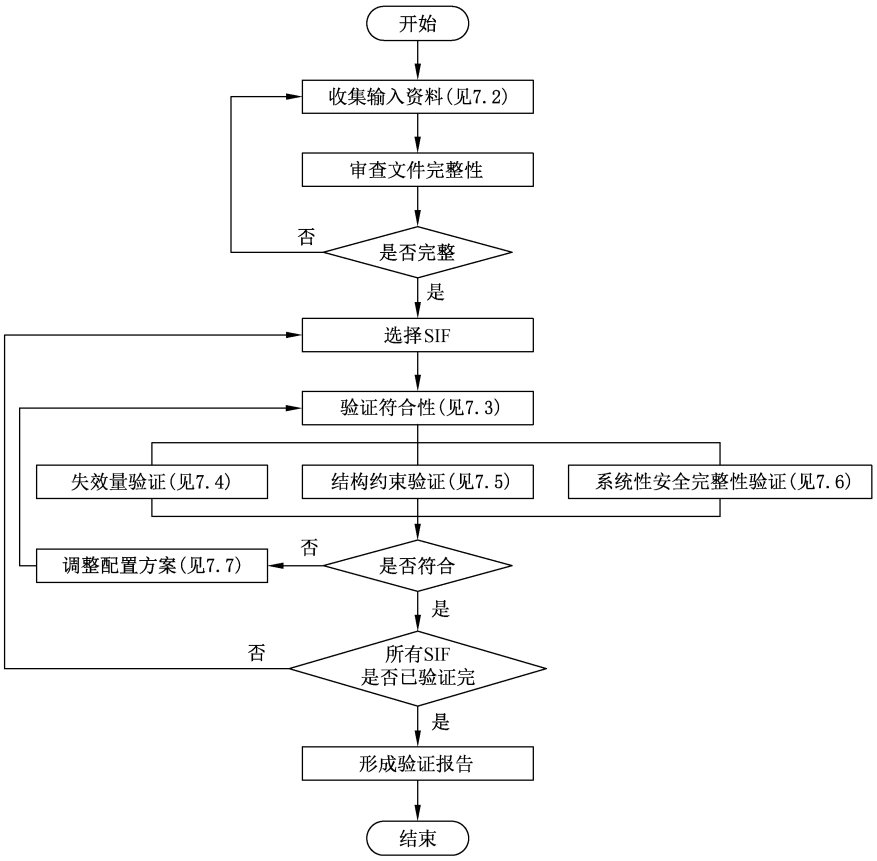


图 3 SIL 验证流程示意图

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内容：

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；
j) 变更文件。

7.2.2 可检查表的形式检查 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 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 PFD_{avg} 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 应确定用于 SIL 验证的 SIF 目标失效量。SIL 定级给出明确的目标失效量时,SIF 目标失效量应采用此目标失效量。SIL 定级没有给出明确的目标失效量,只给出 SIL 等级时,SIF 目标失效量参考表 3 或表 4,可采用要求达到的 SIL 等级对应的最小的 PFD_{avg} 或 PFH。

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 PFD_{avg} 或 RRF 衡量,根据表 3 确定。

表 3 安全完整性等级(低要求操作模式)

SIL	PFD_{avg}	RRF
4	$\geqslant 10^{-5}$ 到 $< 10^{-4}$	>10 000 到≤100 000
3	$\geqslant 10^{-4}$ 到 $< 10^{-3}$	>1 000 到≤10 000
2	$\geqslant 10^{-3}$ 到 $< 10^{-2}$	>100 到≤1 000
1	$\geqslant 10^{-2}$ 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,SIF 的 SIL 等级应采用 PFH 衡量,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	$\geqslant 10^{-9}$ 到 $< 10^{-8}$
3	$\geqslant 10^{-8}$ 到 $< 10^{-7}$
2	$\geqslant 10^{-7}$ 到 $< 10^{-6}$
1	$\geqslant 10^{-6}$ 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(如传感器、逻辑解算器及最终元件),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 3 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%,并且失效量计算中使用的可靠性数据应由不小于 70%的统计置信区间上限确定;

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
≥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（N＝1，2，3）应满足 SIF 要求的 SIL 等级要求。设备的系统性能力 SC N 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—2017）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—2017）；

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 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，不准许继续增加 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，可采取的措施例如：

a）　选择高可靠性设备；

b）　提高冗余配置；

c） 缩短 TI(如适用)；
d） 提高检验测试覆盖率；
e） 减少共因失效；
f） 增加 PST 功能；
g） 重新进行安全评估,考虑是否可通过增加保护层来降低 SIL 等级要求。

7.7.2 调整输入及对验证的影响见附录 D。

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） 对于验证不合格的 SIF 给出的建议措施(尤其是对现役装置进行 SIL 验证时)；
f） SIL 验证结果清单和建议清单。

7.9 验证示例

7.9.1 SIL 验证的示例见附录 A。

7.9.2 附录 A 以实际的 SIF 为例,采用计算软件,详细具体地执行了 SIL 计算和验证,包括如下内容。
a） 明确 SIF 的结构以及表决关系。根据 SIL 定级报告中的 SIF 描述、P&ID、逻辑描述和相关设计文件,确定 SIF 各子系统(传感器、逻辑解算器、最终元件)组成的逻辑表决结构。
b） 整理 SIF 组件的失效数据。明确数据来源、组件的安全失效 $\lambda_{SD}/\lambda_{SU}$、危险失效 $\lambda_{DD}/\lambda_{DU}$ 等。
c） 整理每个子系统及组件的以下参数：
- 采用的标准(本例中,使用 GB/T 21109.1—2022)；
- 操作模式(低、高或者连续)；
- 使用期限(MT)；
- 检验测试间隔(TI)；
- 检验测试覆盖率(PTC)；
- 共因因子等。

d） 计算 SIF 的 PFD_{avg} 和 STR。
e） 得到整个 SIF 功能回路的 PFD_{avg}、HFT、SC、STR 后,对比要求值,判定该 SIF 回路是否实现 SIL 定级要求。当对 STR 无要求时,不需对比判定。

附 录 A
（资料性）
SIL 验证示例

A.1 输入

SIF 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。

定级要求：PFD_{avg}＜1E-01，SIL1。

工艺流程：见图 A.1。

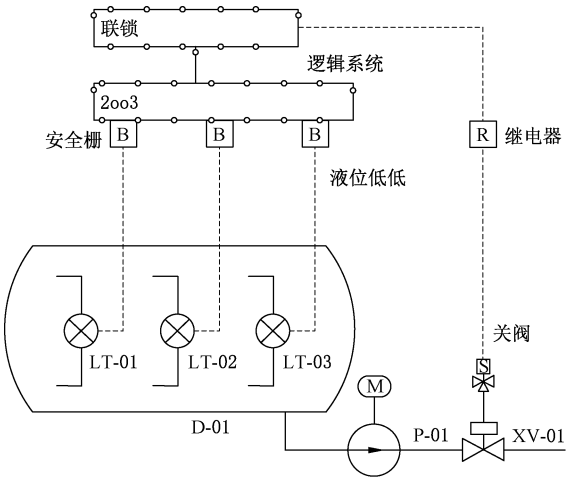


图 A.1 工艺流程

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：

- 传感器子系统，包括：变送器、安全栅等；
- 逻辑解算器子系统，包括：AI、DO、CPU、电源等模块；
- 最终元件子系统，包括：继电器、电磁阀、执行机构、阀门等。

传感器包括了 3 个液位测量仪表，LT-01/02/03，表决关系为 2oo3，任意两个仪表低低联锁即触发联锁动作；逻辑解算器为 SIL3 认证的 SIS 系统；最终元件执行联锁动作，关闭一个阀门。

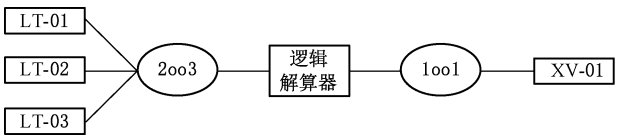


图 A.2 SIF 结构

输入参数 整体部分：

- MT＝10 年；
- TI＝8 760 h（12 个月）；

- PTC＝90％(为简化示例,按全部组件相同考虑)；
- MTTR＝8 h；
- 操作模式: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

子系统	SFF	β	HFT
传感器	87.2％	5％	1
逻辑解算器	97.8％	2％	1
最终元件	63.9％	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	分类	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	备注
传感器	LT-01/02/03	液位变送器	B 类	280	125	774	108	
		安全栅	A 类	0	650	0	350	
逻辑解算器	SIS 系统	CPU 处理器	B 类	7 430	75	2 380	125	
		电源		2 250	0	250	0	
		AI 模块		990	10	900	100	
		AI 通道		48	3	48	300	
		DO 模块		760	40	190	10	
		DO 通道		139	1	57	3	
最终元件	XV-01	继电器	A 类	0	900	0	600	
		电磁阀	A 类	0	300	0	200	
		执行机构	A 类	0	400	0	300	
		球阀	A 类	0	250	0	600	

注 1:λ 的单位为 FIT(10^{-9}次/h)。

注 2:设备分类来自证书、通用数据。

注 3:数据来自证书或通用数据,并为示例的方便作了简化和调整。

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 在使用年限内的变化趋势,及其平均值 PFD_{avg}。

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 PFD_{avg}/SIL 等级		＜1E-01/SIL1		
实现 PFD_{avg}/SIL 等级		1.51E-02/SIL1		
SIF 及子系统	PFD_{avg}	$MTTF_{SP}$/年	实现的 SIL(AC 和 SC 部分)	
			SIL AC	SIL SC
SIF 回路整体	1.51E-02	33.83	2	1
传感器	4.55E-04	499.81	3(HFT＝1)	1
逻辑解算器	2.51E-05	287.91	3(HFT＝1)	3
最终元件	1.46E-02	41.53	2(HFT＝0)	1

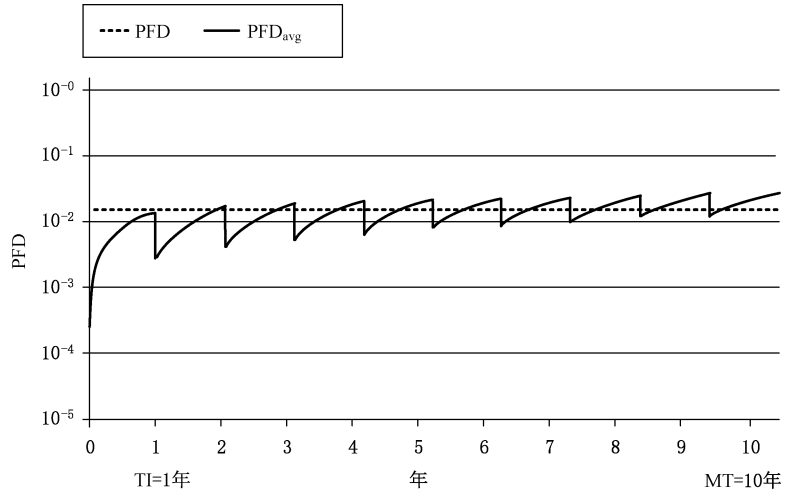


图 A.3　PFD_{avg}趋势图

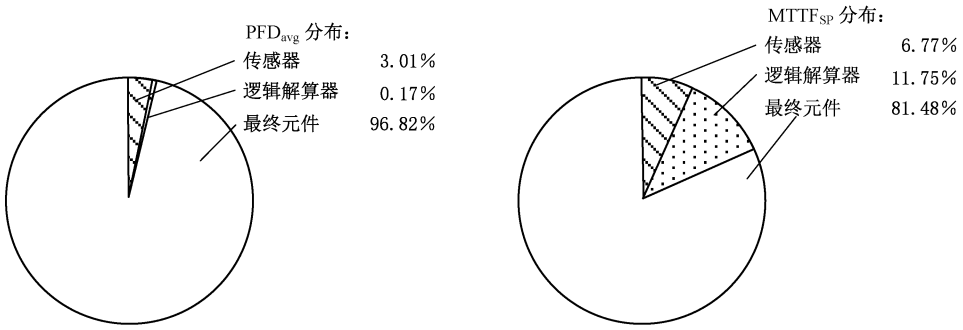


图 A.4　各子系统 PFD_{avg}和 $MTTF_{SP}$分布图

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

序号	输入文件	文件的内容	必须	补充	备注
1-1	SIL 定级报告	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 证书/FMEDA 报告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	联锁逻辑说明与配置，或联锁逻辑图，或逻辑因果表	SIF 配置方案			
4-2		表决关系(MooN)			
5-1	仪表索引、仪表规格书或仪表台账	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“以往使用”的做法时，SIL 证书不是必需的。
注 2：由业主填写汇总传感器、逻辑解算器、最终元件等的信息。
注 3：所有文件需是最新版本。

附 录 C
（资料性）
计算方法

C.1 概述

C.1.1 本附录说明验证涉及的计算方法和概念。本附录及附录 E～附录 H 中的数据和公式来自 ISA TR84.00.02—2022。

C.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。其中的计算涉及仪表的可靠性数据管理、目标管理、工作环境，例如：有效的仪表供电、布线等安全设计。

C.1.3 SIF 计算的内部过程见图 C.1。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，详细见后续条款。其中：计算输入见 C.2；计算过程见 C.3～C.7；特殊的其他问题见 C.8。

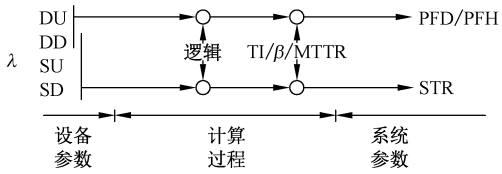


图 C.1 SIF 计算

C.1.4 PFD 的整体计算过程如下。

一个 SIF 包括 3 个部分：

a) 传感器(E)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。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(LS)部分：包括输入、控制器、输出等。

c) 最终元件(FE)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。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_{avg}。合并 3 部分求和，即 SIF 的 PFD_{avg}。对于 ETT 系统，需增加考虑支持系统(SS)的电源的失效。详见公式(C.1)：

$$PFD_{SIF} = PFD_S + PFD_{LS} + PFD_{FE} + PFD_{SS} \quad \cdots\cdots\cdots\cdots\cdots\cdots (C.1)$$

注：公式(C.1)中的所有 PFD 均指 PFD_{avg}。

PFH、STR 的过程相同。支持系统对于 STR 计算适用不同的原则。

C.2 失效的基本特征

C.2.1 本条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 中 3.3 的注 2。

C.2.2 失效的分级见表 C.1。

表 C.1　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

C.2.3　失效的模式见表 C.2。

表 C.2　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

C.2.4　失效的机理见表 C.3。

表 C.3　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

C.2.5　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 证书的数据应基于分析,并可被查证。表 C.4 罗列了参考数据的部分来源。

表 C.4　数据来源

组织	出版物、手册	网址
PERD Process Equipment Reliability Database	—	http://www.aiche.org/CCPS/ActiveProjects/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	—

C.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 β。例如：2 个冗余的变送器，隔膜被水锤损坏，同时故障，是共因故障。而其中 1 个的电路损坏，是独立失效。

C.2.7　失效的详细分级（安全\危险失效、是否检测到的失效，以及与“被揭露出”的关系）见图 C.2。

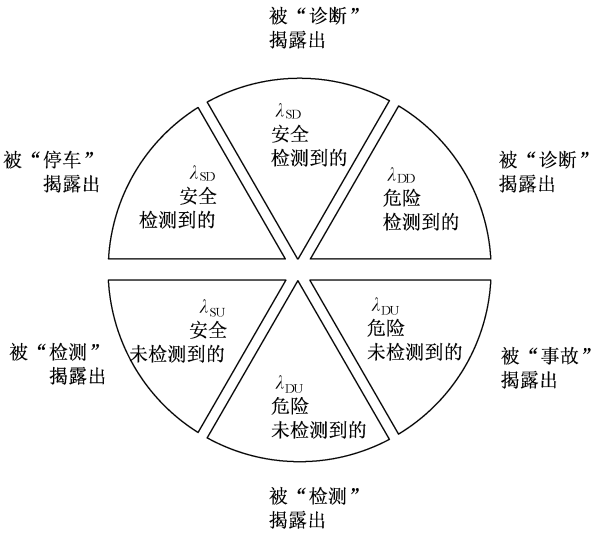


图 C.2　失效详细分级

C.2.8　设备失效率参数的关系如下，示意见图 C.3。

λ 分为 4 部分：λ_{DU}、λ_{DD}、λ_{SU}、λ_{SD}。

λ_D 是 λ_{DU} 和 λ_{DD} 之和，λ_S 是 λ_{SU} 和 λ_{SD} 之和。

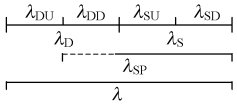
λ_{SP} 包含 λ_S，λ_{SP} 是否还包含 λ_{DD} 取决于系统设计（检测到的危险失效是否可安全停车）。通常认为失电停车 DTT 系统的 λ_{SP} 包含 λ_{DD}；反之，ETT 时不包含。

DC 是 λ_D 中 λ_{DD} 的比例。

SFF 是 λ 中 λ_{SP} 的比例。

λ 是 MTTF 的倒数。

MTBF 是 MTTF 和 MTTR 之和，通常 MTTF 远远大于 MTTR，所以 MTBF 约等于 MTTF。



$DC=\lambda_{DD}/\lambda_D$

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

$\lambda=1/MTTF$

MTBF＝MTTF＋MTTR≈MTTF（MTTF远大于MTTR）

图 C.3　设备失效率

C.2.9　设备的失效率服从浴盆效应，见图 C.4。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 验证仅计算使用期的稳定的随机失效。

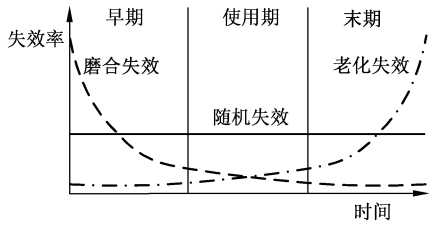


图 C.4　浴盆效应

C.3　操作模式

C.3.1　SIF 的操作模式见表 C.5。

表 C.5　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。 验证：PFD_{avg}	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。 验证：PFH	批量反应器进料超限： 每批次：16 h 运行，4 h 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。 验证：PFH	反应器温度： 温度控制应维持正常；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。		

C.3.2　SIL 验证的输入文件应明确每个 SIF 的操作模式、验证选择（PFD_{avg} 或 PFH）、目标值。

C.3.3　PFD_{avg} 是一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）。选择目的是更客观地反映实际情况。

C.3.4　STR 的验证仅考虑瞬时情况，不考虑操作模式和 DR。

C.4 PFH 计算

C.4.1 PFH 的一般公式见公式(C.2)。

$$PFH_{MooN}=\frac{N!}{(N-M)!\ (M-1)!}\times(1-\beta)\times\lambda_D\times\left(\frac{(1-\beta)\times\lambda_D\times TI}{2}\right)^{N-M}+(\beta\times\lambda_D) \quad \cdots\cdots\cdots\cdots(C.2)$$

公式的说明如下：

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。

C.4.2 PFH 具体公式和推导见附录 E。

C.5 PFD 计算

C.5.1 本条详细说明 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 计算各条不再详述，参考 PFD 计算。

C.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 C.5，3 个部分的任 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：传感器 2 取 1，最终元件 2 取 1)见图 C.6，2 个传感器(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。

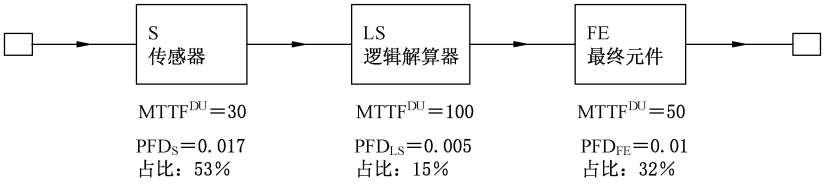


图 C.5 可靠性方块图(单表结构)

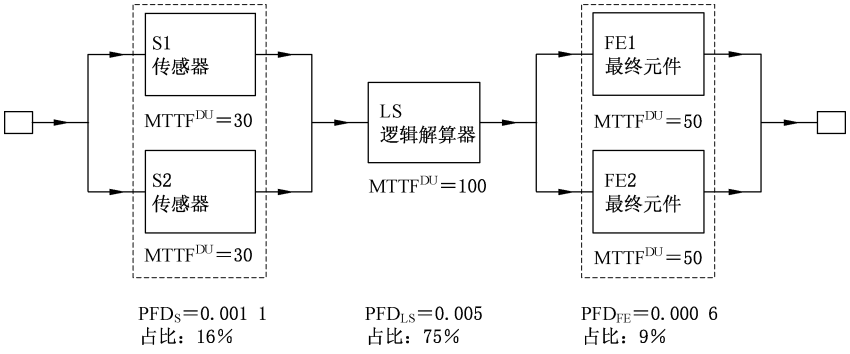


图 C.6 可靠性方块图(冗余结构)

C.5.3 完整的维修时间指：从失效停止工作，到校正后再次工作，之间的不可工作时间。见图 C.7，包括：

a) 检测失效的时间；

b) 开始维修前的准备时间；

c） 实际的维修时间；

d） 组件恢复运行前的等待时间。

相关的定义及依据如下：

- MTTR(平均恢复时间 mean time to restoration)指 a、b、c、d 部分；
- MRT(平均维修时间 mean repair time)指 b、c、d 部分；
- 因历史原因，MTTR 也被用作平均维修时间(mean time to repair)，即 MRT；
- MTTR 参与 SIF 计算，对结果影响比较小。

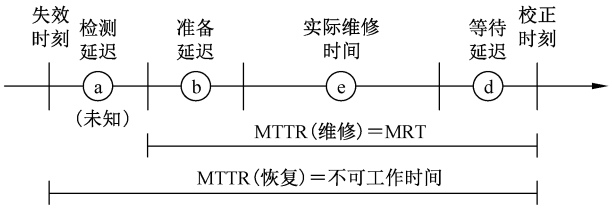


图 C.7 MTTR

C.5.4 表决(*N* 取 *M*)逻辑影响了(单个仪表和组合之间的)失效传递关系，见表 C.6。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 C.6 表决

表决	危险 HFT	安全 HFT	逻辑图
1 取 1	0	0	1取1；2取1；2取2；3取2；4取2
2 取 1	1	0	
2 取 2	0	1	
3 取 2	1	1	
4 取 2	2	1	

C.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(例如：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 C.8。

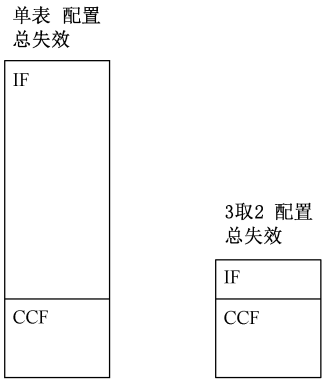


图 C.8 共因

C.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，以及 PFD 具体公式见附

录 F 和附录 G。

C.6 STR 计算

C.6.1 STR 的一般公式见公式(C.3)。

$$STR_{MooN} = N!\ /\ [R!\ (M-1)!\ ] \cdot R \cdot \lambda_{sp} \cdot [\lambda_{sp} \cdot (TI/2 + MTTR)]^{M-1} \quad \cdots\cdots (C.3)$$

公式的说明如下：

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。

C.6.2 STR 的具体公式见附录 E。

C.7 SIF 计算

C.7.1 基于以下假设，可把实际实现理想化为数学模型，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(λ_{DD})发生时，将发生安全停车。

h) 人员经过培训，按照制度工作。

C.7.2 SIF 计算仅针对随机失效。系统失效无法被定量计算，需整体估算。

C.7.3 不同方法的 SIF 计算示例及比较见附录 H。

C.8 其他

C.8.1 冗余结构中，各个设备的失效率不同时，采用表 C.7 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 表决时，每个变送器的 λ 不同，采用第 3 列替换第 1 列，修正原公式。

表 C.7 不同失效率的公式调整

相同失效率	不同失效率：2 取 M 时	不同失效率：3 取 M 时
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	—	$\lambda_1\lambda_2\lambda_3$

C.8.2 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。

C.8.3 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。

C.8.4 通过查表法计算 PFD，可参考 GB/T 20438.6—2017 中附录 B 的 B.3.2.3。

C.8.5 PTC（检验测试覆盖率）对 PFD_{avg} 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。

C.8.6 对于提高可靠性的冗余配置（例如：2 取 1、3 取 2 等），β 影响 PFD_{avg}，说明如下。

a） 对影响因素综合评分后，β 取值宜在 10％以内。

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（例如：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、文档管理、维护制度、专业化、运行环境等多因素影响。例如：（不同测量方法、相同测量方法但不同制造厂、相同测量方法和制造厂）的传感器：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 中表 D.4。

C.8.7 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。

C.8.8 “以往使用”的做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。

C.8.9 FMEA 列表分析失效的模式、分级、原因、机理。例子见附录 I。

附 录 D
（资料性）
调整和影响

SIL 验证计算时，调整输入参数对结果的影响，见表 D.1。

表 D.1 调整和影响

对象	调整	措施	可靠性 PFD/PFH	可用性 STR	经济性 成本	备注
共因 β	降低	采购不同制造厂的产品	提高	提高	不变	
		完善设计、健全管理	提高	提高	不变	
	提高	不采取额外措施	降低	降低	不变	
产品可靠性 λ	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 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	小量降低	提高	提高	
		2oo2 改为 2oo3	提高	小量降低	提高	
	降低	2oo3 改为 1oo2	小量提高	降低	降低	
		2oo3 改为 2oo2	降低	小量提高	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	
检验测试间隔（TI）	缩短		提高	不变	提高	
	延长		降低	不变	降低	
平均恢复时间（MTTR）	缩短		不变	提高	提高	影响小
	延长		不变	降低	降低	影响小
使用期限（MT）	缩短		提高	提高	提高	
	延长		降低	降低	降低	
检验测试覆盖率（PTC）	提高		提高	提高	提高	
	降低		降低	降低	降低	

补充说明：针对验证不合格的情况，还有其他应对策略。例如：考察该 SIF 设置的科学性和合理性。检查并分辨动作是否与安全相关。

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。

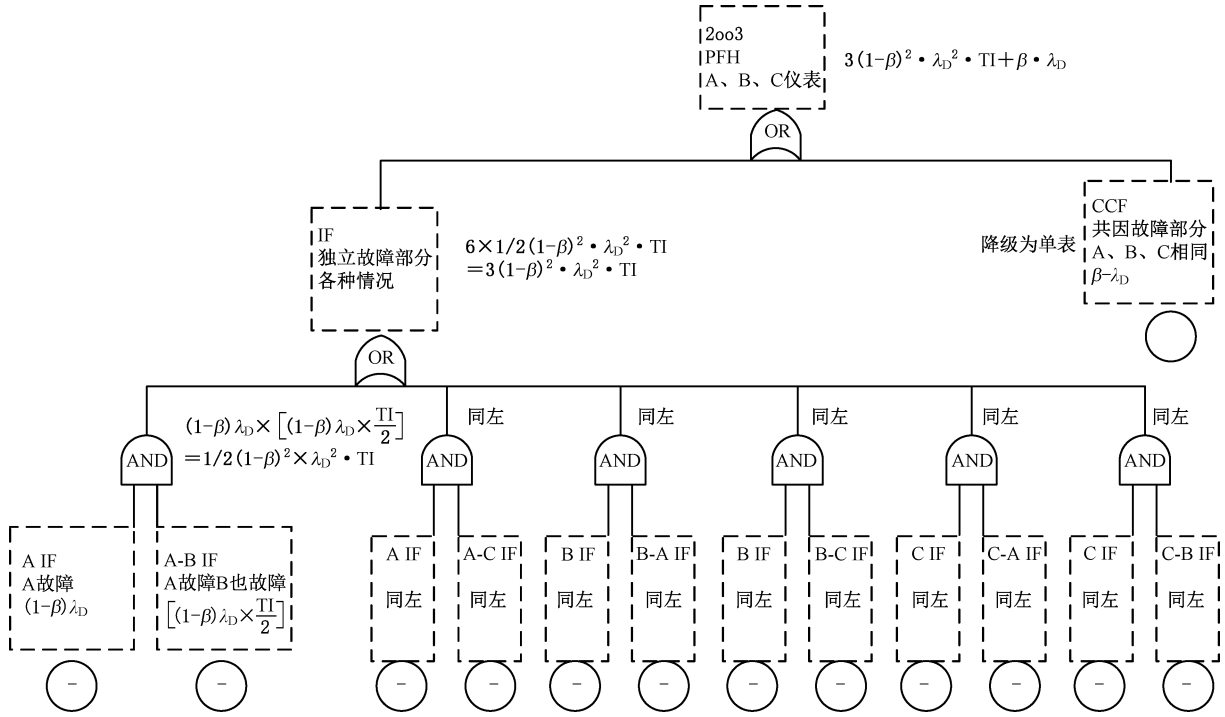


图 E.1 PFH 失效模型

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
1 取 1	λ_D
2 取 1	$(1-\beta)^2 \cdot \lambda_D^2 \cdot TI+\beta \cdot \lambda_D$
3 取 1	$3/4 \cdot (1-\beta)^3 \cdot \lambda_D^3 \cdot TI^2+\beta \cdot \lambda_D$
2 取 2	$2\lambda_D$
3 取 2	$3(1-\beta)^2 \cdot \lambda_D^2 \cdot TI+\beta \cdot \lambda_D$
3 取 3	$3\lambda_D$
注：公式的适用条件、参数调整见正文章条。	

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	0.034	0.013	0.000 22	0.004 7
3 取 1	0.001 1	0.003 2	0.000 16	0.000 17
2 取 2	0.1	0.1	0.016	0.016
2 取 3	0.008 2	0.037	0.000 34	0.001 1
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：$\beta=2\%$。

E.2　PFD 基本公式的推导

结论：对于单个设备，$PFD_{avg}=\lambda \cdot TI/2$。

推导过程：见 ISA TR84.00.02—2022 的附录 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：$e^{-\lambda t}$。
- PFD_{avg} 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：$PFD_{avg}=\lambda \cdot TI/2$。

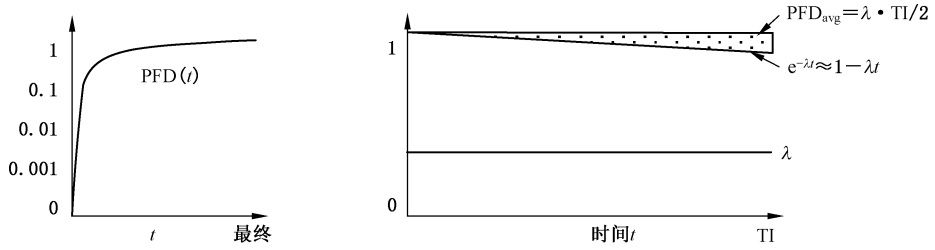


图 E.2　PFD 示意

PFD 的具体公式见附录 F 和附录 G。

E.3　STR 公式

STR 的公式见表 E.3。

表 E.3　STR 公式

配置	公式
1 取 1	λ_{sp}
2 取 1	$2\lambda_{sp}$

表 E.3　STR 公式（续）

配置	公式
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、参数调整见正文章条。	

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 20 世纪 60 年代，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。20 世纪 70 年代，扩展至核工业，用于估算核反应堆失控的可能性。20 世纪 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

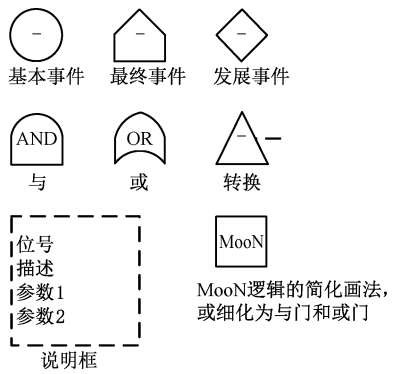


图 F.1 FTA 图例

F.3 公式

故障树法的 PFD_{avg} 一般公式见公式(F.1)。

$$PFD_{avg}=N!/(R!(M-1)!)\cdot((1-\beta)\cdot((1-DC)\cdot\lambda_D\cdot TI/2+DC\cdot\lambda_D\cdot DI/2+\lambda_D\cdot MTTR)^R+\beta\cdot((1-DC)\cdot\lambda_D\cdot TI/2+DC\cdot\lambda_D\cdot DI/2+\lambda_D\cdot MTTR) \quad \cdots\cdots(F.1)$$

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$(1-\beta)$系数的部分。

故障树法的 PFD_{avg} 具体公式见表 F.2。

表 F.2 故障树法的 PFD_{avg} 近似公式

配置	公式
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。

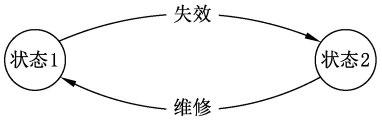


图 G.1 简单模型

状态 1 是在正常运行的原件状态。状态 2 是故障但可修复的原件的状态。正常运行状态可失效，转换为状态 2；故障但可修复的状态经过维修，转换为状态 1。

G.2 建模原理

G.2.1 建模说明

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。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，分析人员可只关注模型的构建，而不是基础的数学运算。不过，至少理解本附录所介绍的方法原理。关于马尔可夫方法更详细地讨论，读者可参考 ISO/TR 12489：2013。

故障安全和故障危险模式的马尔可夫模型见图 G.2。

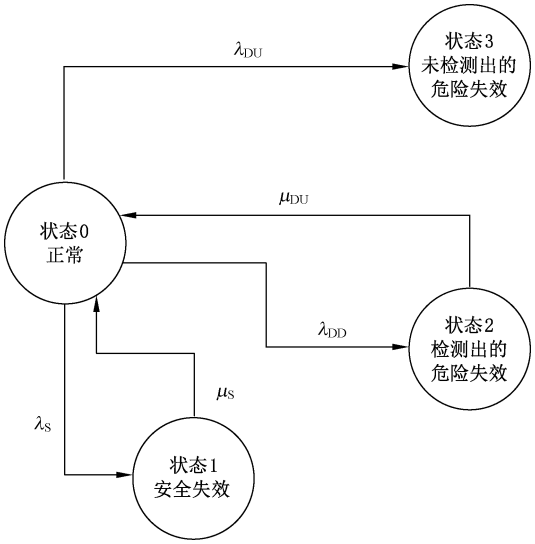


图 G.2　故障安全和故障危险的马尔可夫图

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.2.2　建模过程

建模过程主要分为以下 3 个部分。

a）　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。

b）　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。

c）　计算状态之间转换的概率。

状态 0--〉状态 1　安全失效率 λ_S；

状态 0--〉状态 2　检测出的危险失效率 λ_{DD}；

状态 0--〉状态 3　未检测出的危险失效 λ_{DU}；

状态 1--〉状态 0　安全失效修复率 μ_S；

状态 2--〉状态 0　检测出的危险失效修复率 μ_{DD}。

G.2.3　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 $N\times N$ 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 4×4 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	$1-\lambda_S-\lambda_{DD}-\lambda_{DU}$	λ_S	λ_{DD}	λ_{DU}
1	μ_S	$1-\mu_S$	0	0
2	μ_{DD}	0	$1-\mu_{DD}$	0
3	0	0	0	1

已知 $\lambda_S=0.001$，$\mu_S=0.04$，$\lambda_{DD}=0.06$，$\mu_{DD}=0.125$，$\lambda_{DU}=0.03$，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.2.4　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公式(G.1)来表示：

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

式中：

$P(t)$——时刻 t 的状态概率向量；

t　——时刻 t，单位为小时(h)；

$[M]$——状态转移概率的马尔可夫矩阵；

$P(0)$——初始状态概率向量，通常为一个列向量，完好状态为 1，其他状态为 0。

尽管矩阵指数的属性与普通指数不完全相同，也可得出公式(G.2)：

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

式中：

$P(t)$ ——时刻 t 的状态概率向量；

t　——时刻 t，单位为小时(h)；

t_1　——上一时刻 t_1，单位为小时(h)；

$[M]$ ——状态转移率的马尔可夫矩阵；

$P(0)$ ——初始状态概率向量，通常为一个列向量，完好状态为 1，其他状态为 0；

$P(t_1)$——时刻 t_1 状态向量，通常为一个列向量。

以上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。

通过公式(G.2)可得出前 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	0.000 0	0.000 0	0.000 0
1	0.909 0	0.001 0	0.060 0	0.030 0
2	0.833 8	0.001 9	0.107 0	0.057 3
3	0.771 4	0.002 6	0.143 7	0.082 3
4	0.719 3	0.003 3	0.172 0	0.105 4
5	0.675 4	0.003 9	0.193 7	0.127 0
6	0.638 3	0.004 4	0.210 0	0.147 3
7	0.606 7	0.004 9	0.222 0	0.166 4
8	0.579 4	0.005 3	0.230 7	0.184 6
9	0.555 7	0.005 6	0.236 6	0.202 0

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 PFD_{avg} 是所有 PFD 的平均值。

PFD_{avg} 可通过平均累计时间（MCT）进行计算，见公式（G.3）和（G.4）。

$$\overrightarrow{MCT}(T)=\int_0^T \vec{P}(t)\,dt \qquad \cdots\cdots(G.3)$$

式中：

MCT ——状态平均累计时间向量；

T ——最终时刻 T，单位为小时（h）；

$P(t)$ ——时刻 t 的状态概率向量。

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：

$$PFD_{avg}(T)=\frac{1}{T}\sum_{k=1}^{n} q_k MCT_k(T) \qquad \cdots\cdots(G.4)$$

式中：

T ——最终时刻 T，单位为小时（h）；

n ——状态总数量，单位为个；

q_k ——状态变量，如果系统在状态 k 时为不可用，则 $q_k=1$，在其他情况下 $q_k=0$。

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、不完善地测试和修复、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 PFD_{avg} 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”PFD_{avg}公式

配置	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	$\left[\begin{array}{l}\frac{1}{3}\ [(1-DC)\times(1-\beta)\times\lambda_D\times TI]^2+\\(1-DC)\,DC\times[(1-\beta)\times\lambda_D]^2\times TI\left(\frac{DI}{2}+MTTR\right)\end{array}\right]+\left[\begin{array}{l}\frac{(1-DC)\times\beta\times\lambda_D\times TI}{2}+\\\frac{DC\times\beta\times\lambda_D\times DI}{2}+\beta\times\lambda_D\times MTTR\end{array}\right]$
3 取 1	$\left[\begin{array}{l}\frac{1}{4}\ [(1-DC)\times(1-\beta)\times\lambda_D\times TI]^3+\\(1-DC)^2DC\times[(1-\beta)\times\lambda_D]^3\times TI^2\left(\frac{DI}{2}+MTTR\right)\end{array}\right]+\left[\begin{array}{l}\frac{(1-DC)\times\beta\times\lambda_D\times TI}{2}+\\\frac{DC\times\beta\times\lambda_D\times DI}{2}+\beta\times\lambda_D\times MTTR\end{array}\right]$
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	$\left[\begin{array}{l}[(1-DC)\times(1-\beta)\times\lambda_D\times TI]^2+\\3\times(1-DC)\,DC\times[(1-\beta)\times\lambda_D]^2\times TI\left(\frac{DI}{2}+MTTR\right)\end{array}\right]+\left[\begin{array}{l}\frac{(1-DC)\times\beta\times\lambda_D\times TI}{2}+\\\frac{DC\times\beta\times\lambda_D\times DI}{2}+\beta\times\lambda_D\times MTTR\end{array}\right]$
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 PFD_{avg}、H.3 计算 STR。

H.2 计算 PFD_{avg}

H.2.1 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 中附录 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 和附录 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	λ_D 1/年	λ_S 1/年	MTTR 小时	CCF	Tau	Q	λ_{DU} 1/年	λ_{DD} 1/年	λ_{DU} FIT	λ_{DD} FIT	λ_{SU} FIT	λ_{SD} FIT
PT	压力变送器	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	停车器件	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	电磁阀	1.67 E-2	3.33 E-2	72	1%	5	4.07 E-2	1.63 E-2	4.20 E-4	1 858	48	3 801	0
BV	关断阀	2.72 E-2	4.38 E-3	72	1%	5	6.52 E-2	2.61 E-2	1.12 E-3	2 977	128	500	0

注 1：原始数据见 ISA TR84.00.02—2022 中附录 H 的表 H.1、图 H.2。

注 2：本表 A 部分罗列了原始数据，B 部分是反算过程，C 部分清理了计算输入数据。

注 3：本表 B 部分中，$\lambda_{DU}=Q/\text{Tau}\times 2$。

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			PFD_{avg}（TI=1 年）			PFD_{avg}（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.2.2	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.2.3	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.2.4	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.2.5	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.2.6	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.2.7	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.2.8	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.2.9	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。

“2 取 1/2 取 2”配置指：整体阀门是 2 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。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义，但不影响可读。

H.2.2 例子：工艺简图见图 H.1，计算图见图 H.2，计算表见表 H.3。

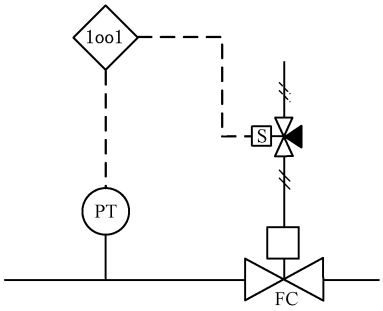


图 H.1 工艺简图

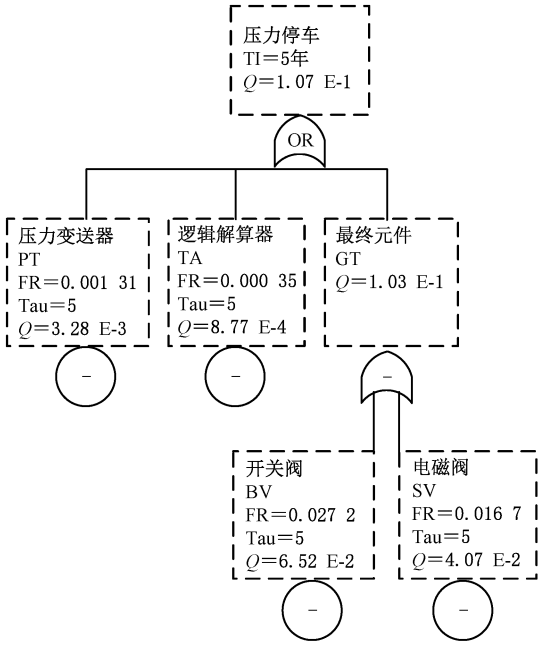


图 H.2 计算图

表 H.3　计算表

总 PFD_{avg}：1.10 E-1												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
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	4 836	串联	SV	1 858

H.2.3　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。

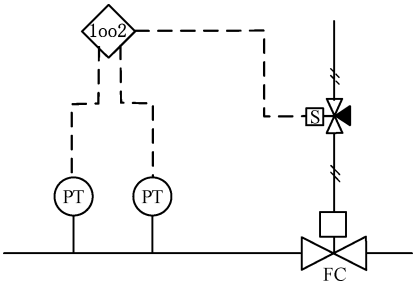


图 H.3　工艺简图

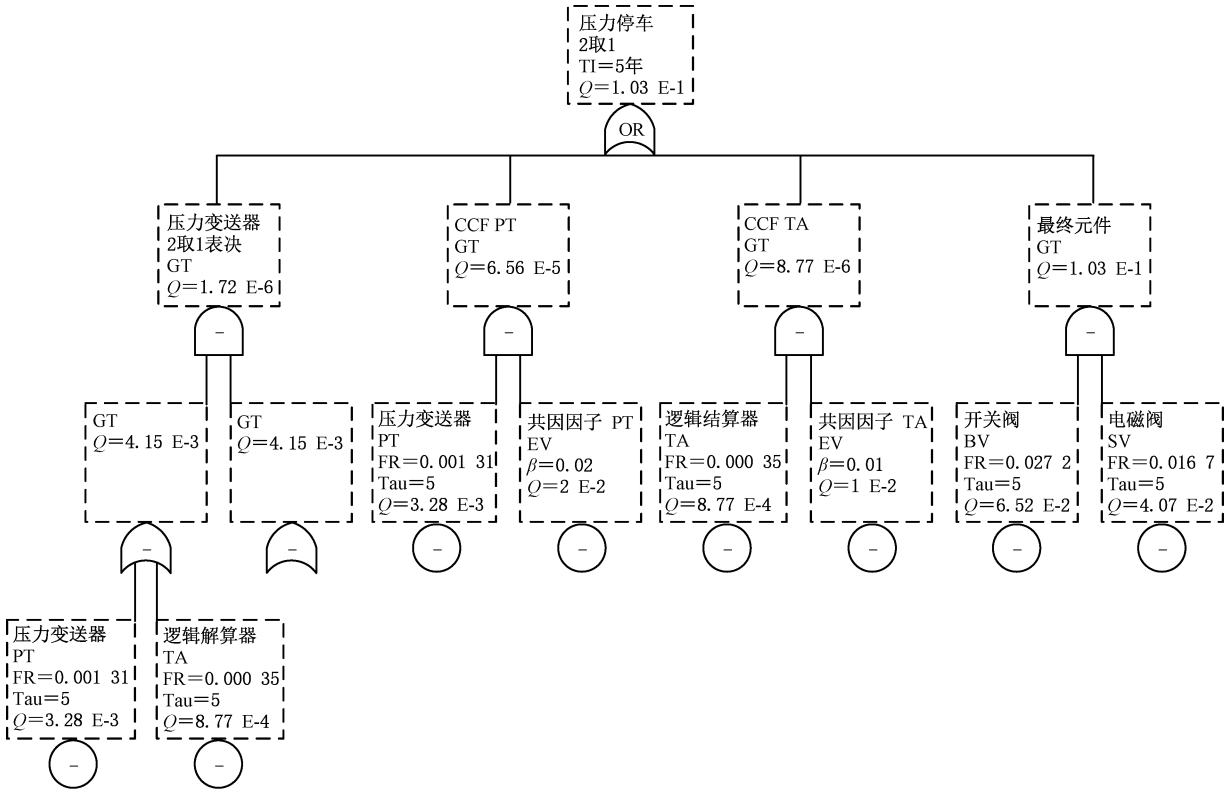


图 H.4　计算图

表 H.4　计算表

总 PFD_{avg}：1.06 E-1												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
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
											TA	40
								PT-2	189	复用		
最终元件	1.1 E-1	等效	阀门					V-1	4 836	串联	SV	1 858
											BV	2 977

H.2.4　例子：工艺简图见图 H.5，计算图见图 H.6，计算表见表 H.5。

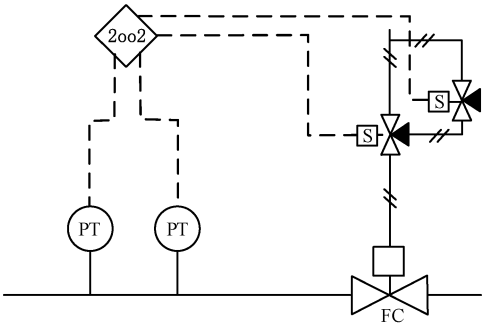


图 H.5　工艺简图

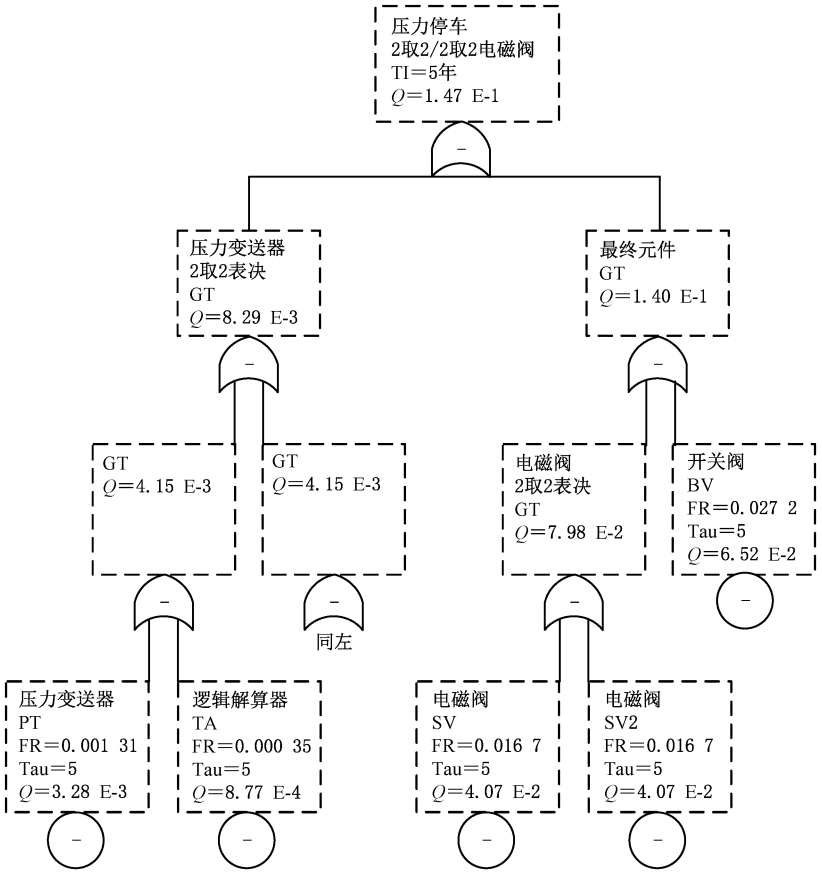


图 H.6　计算图

表 H.5　计算表

总 PFD_{avg}：1.55 E-1												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
传感器	8.3 E-4	等效	测量	8.3E-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	6 694	串联	SV	3 717
											BV	2 977
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	1 858			3 717
				3 717 FIT				SV2	1 858			1 858

H.2.5　例子：工艺简图见图 H.7，计算图见图 H.8，计算表见表 H.6。

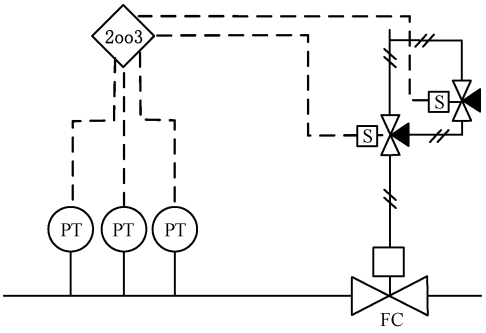


图 H.7　工艺简图

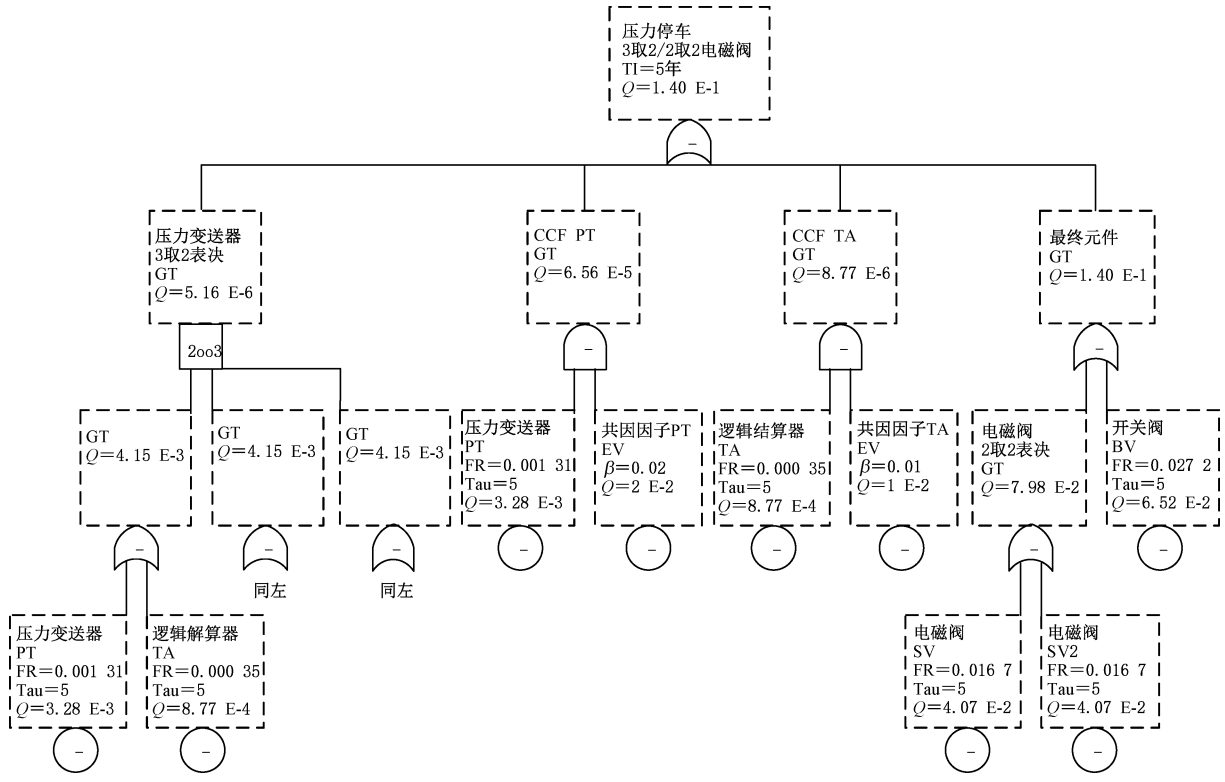


图 H.8　计算图

表 H.6　计算表

总 PFD_{avg}：1.50 E-1												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
传感器	9.6 E-5	等效	测量	9.6 E-5	3 取 2	2%	72	PT-1	150	串联	PT	150
								PT-2	150	复用		
								PT-3	150	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-3	40	复用		
最终元件	1.5 E-1	等效	阀门	1.5 E-1	1 取 1			V-1	6 822	串联	SV	3 717
											BV	3 105
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	1 858			1 858
				3 717 FIT				SV2	1 858			1 858

H.2.6　例子：工艺简图见图 H.9，计算图见图 H.10，计算表见表 H.7。

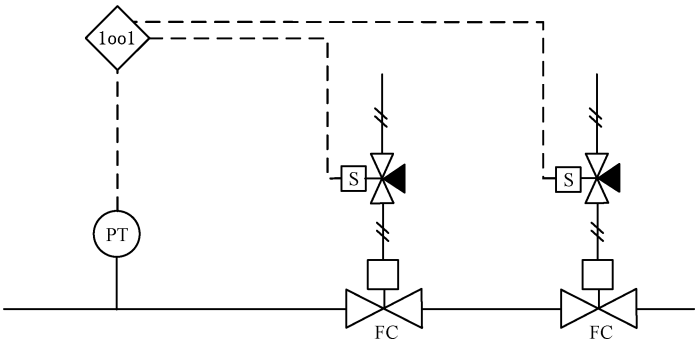


图 H.9　工艺简图

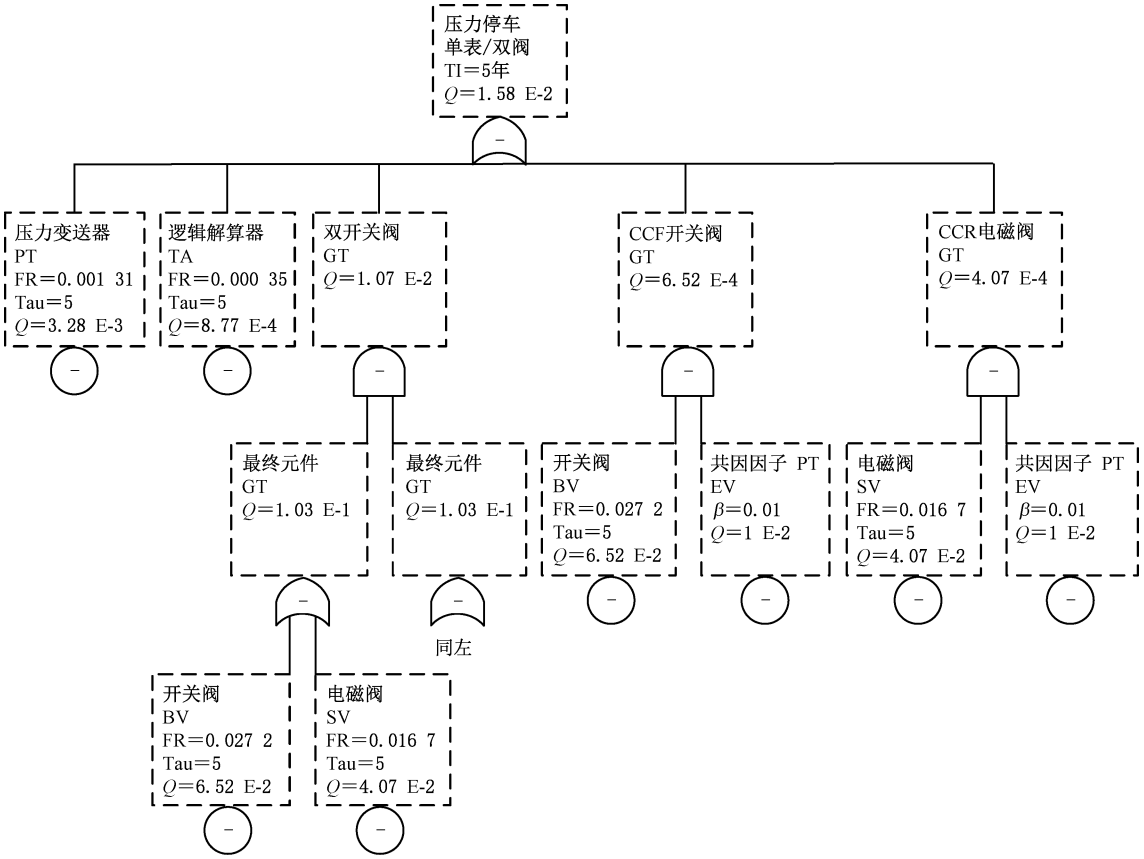


图 H.10　计算图

表 H.7　计算表

总 PFD_{avg}：1.64 E-2												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
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	1.2 E-2	等效	阀门	1.23 E-2	2 取 1	1%	72	V-1	4 836	串联	SV	1 858
											BV	2 977
									4 836	复用		

H.2.7　例子：工艺简图见图 H.11，计算图见图 H.12，计算表见表 H.8。

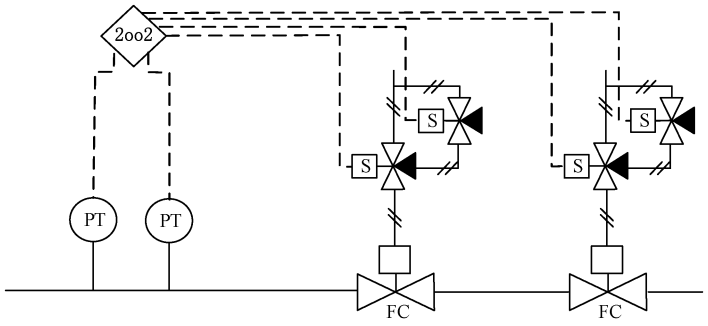


图 H.11　工艺简图

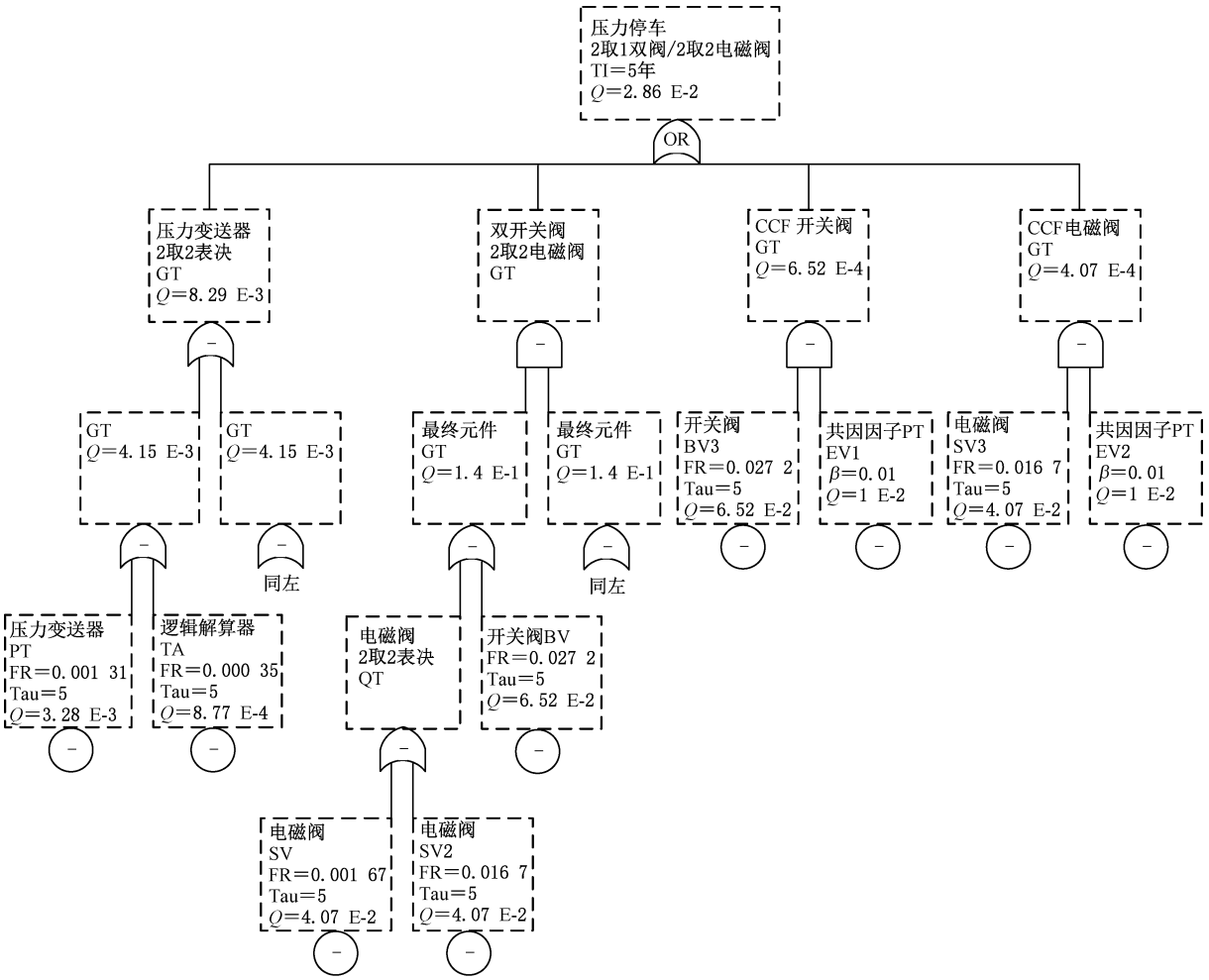


图 H.12　计算图

表 H.8　计算表

总 PFD_{avg}：3.13 E-2												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
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		
逻辑解算器	2.3 E-2	等效	阀门	2.3 E-2	2 取 1	1%	72	V-1	6 694	串联	SV	3 717
											BV	2 977
								V-2	6 694	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	1 858			1 858
				3 717 FIT				SV2	1 858			1 858

H.2.8　例子：工艺简图见图 H.13，计算图见图 H.14，计算表见表 H.9。

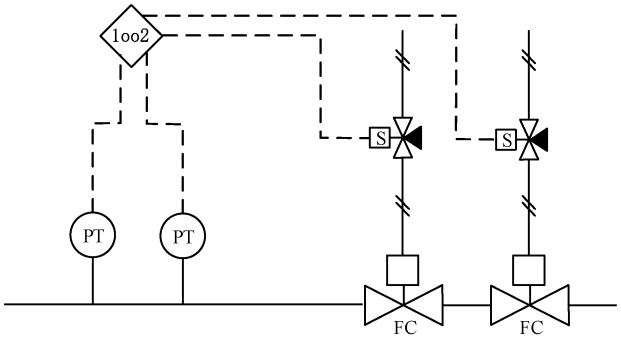


图 H.13　工艺简图

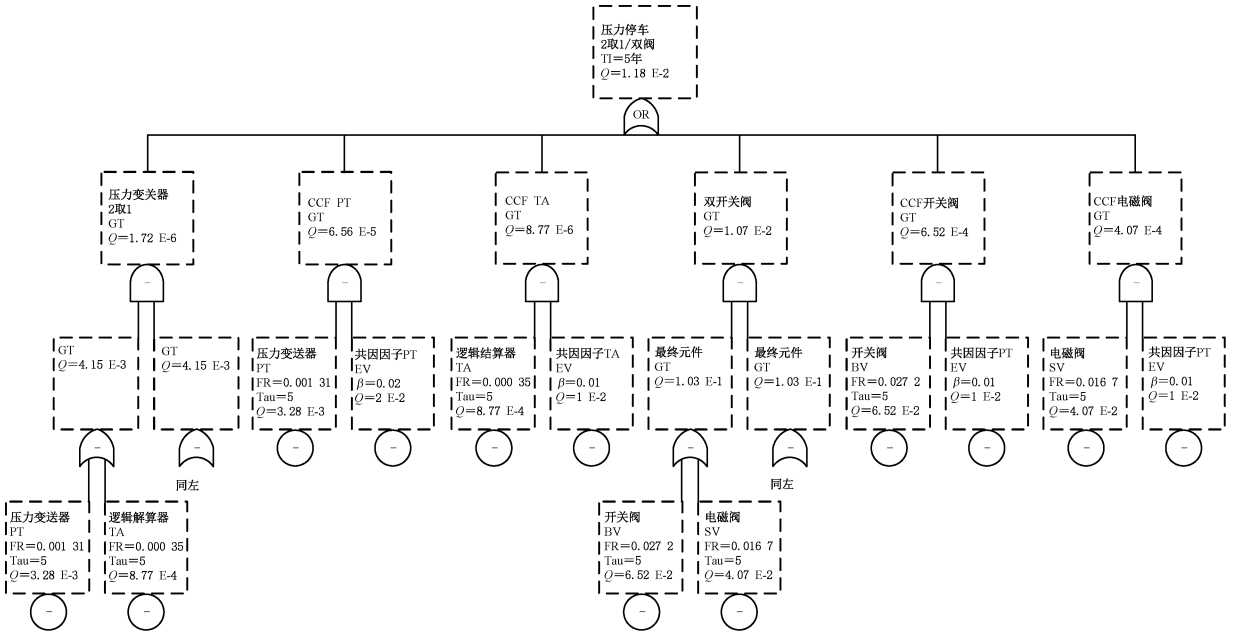


图 H.14　计算图

表 H.9　计算表

总 PFD_{avg}：1.24 E-2												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
传感器	1.0 E-4	等效	测量	1.0 E-4	2 取 1	2% 1%	72	PT-1	189	串联	PT TA	150 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	4 836	串联	SV BV	1 858 2 977
								V-2	4 836	复用		

H.2.9　例子：工艺简图见图 H.15，计算图见图 H.16，计算表见表 H.10。

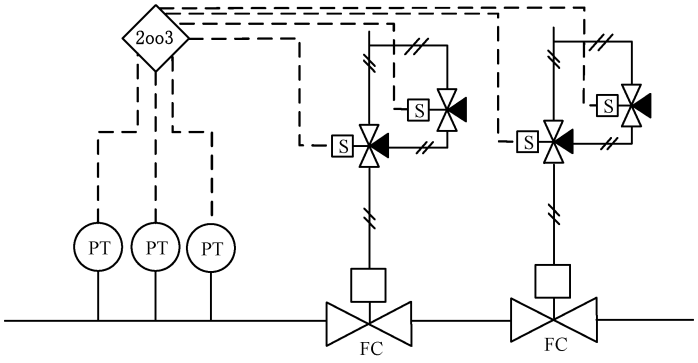


图 H.15　工艺简图

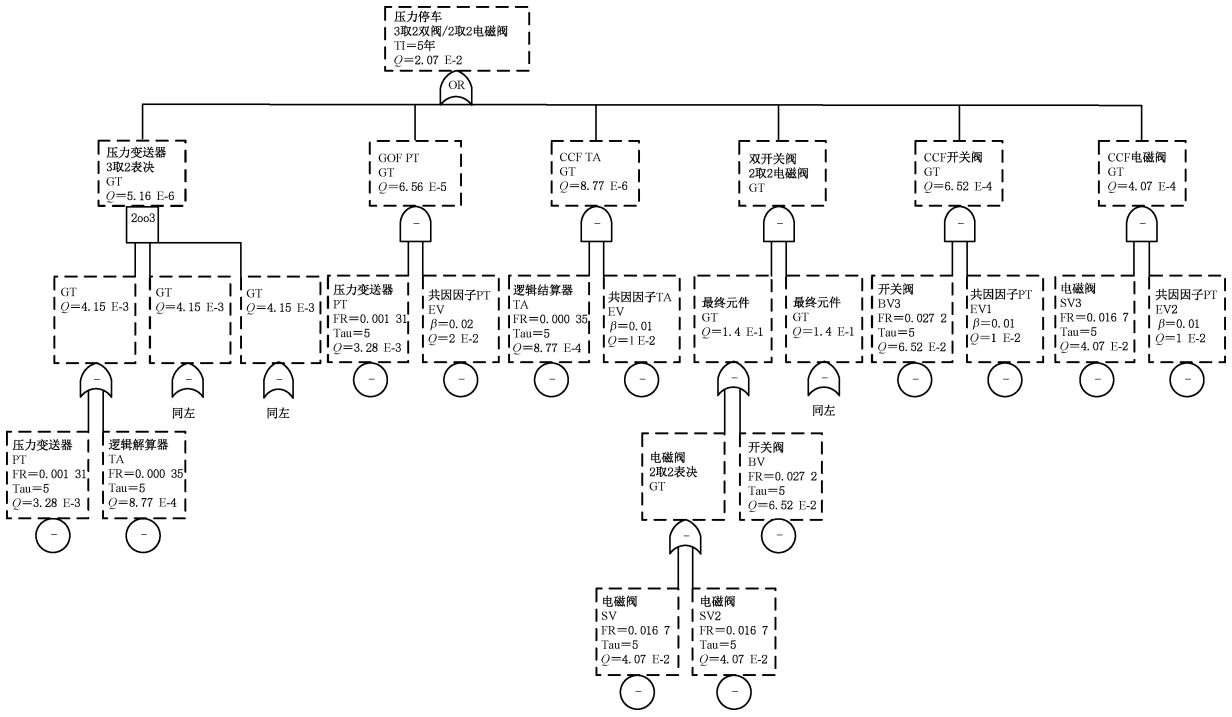


图 H.16　计算图

表 H.10　计算表

总 PFD_{avg}：1.17 E-3												
子系统	PFD_{avg}	配置	部分	PFD_{avg}	配置	β	MTTR 小时	仪表 位号	λ_{DU} FIT	配置	组件 代号	λ_{DU} FIT
传感器	1.9 E-5	等效	测量	1.9 E-5	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	2 取 1	1%	72	V-1	6 694	串联	SV	3 717
											BV	2 977
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	1 858			1 858
				3 717 FIT				SV2	1 858			1 858

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 中附录 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。

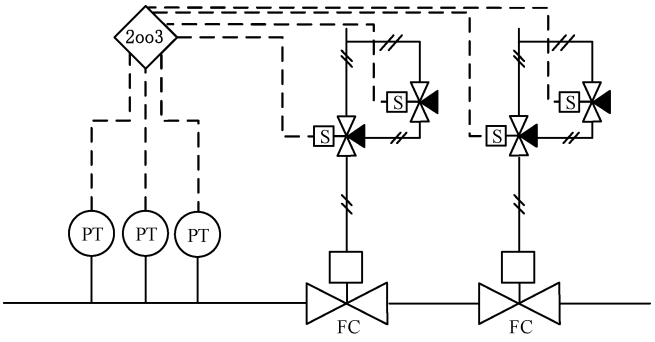


图 H.17　工艺简图

表 H.11　输入数据

表中的数据					反算结果用于使用			
代码	类型	λ_{SP} 次/年	MTTR 小时	CCF	λ_{DU} FIT	λ_{DD} FIT	λ_{SU} FIT	λ_{SD} FIT
PT	压力变送器	1.31 E-3	72	2%			150	
TA	停车器件	3.50 E-3	72	1%			400	
SV	电磁阀	3.33 E-2	72	1%			3 801	
BV	关断阀	4.38 E-3	72	1%			500	
注：TI=5 年。								

表 H.12　计算表

总 STR:2.3 E-6/小时(2.00 E-2/年)												
子系统	STR	配置	部分	STR	配置	β	MTTR 小时	仪表 位号	λ_{SP} FIT	配置	组件 代号	λ_{SP} FIT
传感器	1.3 E-10	等效	测量	1.3 E-10	3 取 2	2%	72	PT-1	549	串联	PT	150
											TA	400
								PT-2	549	复用		
								PT-3	549	复用		
最终元件	2.3 E-6	等效	阀门	2.3 E-6	2 取 1	1%	72	V-1	1 135	串联	SV	635
											BV	500
								V-2	1 151	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	2 取 2	1%	72	SV1	3 801			3 801
				635 FIT				SV2	3 801			3 801

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）
失效模式和影响分析 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
		填充液泄漏	机械损伤、材料腐蚀
		填充液泄漏	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

表 I.1　FMEA 示例（续）

失效模式	失效分级	失效原因	失效机理
电源低	危险	电子故障	错误安装、错误设计
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。			

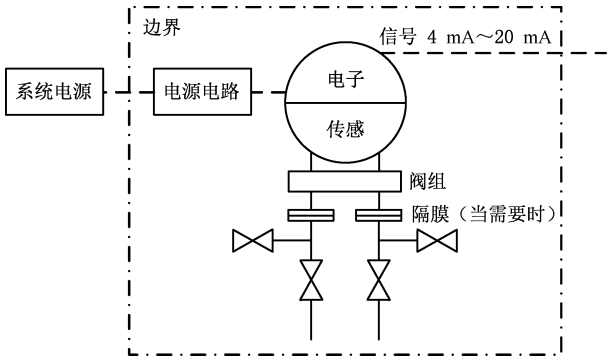


图 I.1　边界图

参 考 文 献

[1] 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

[2] 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

[3] 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

[4] 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