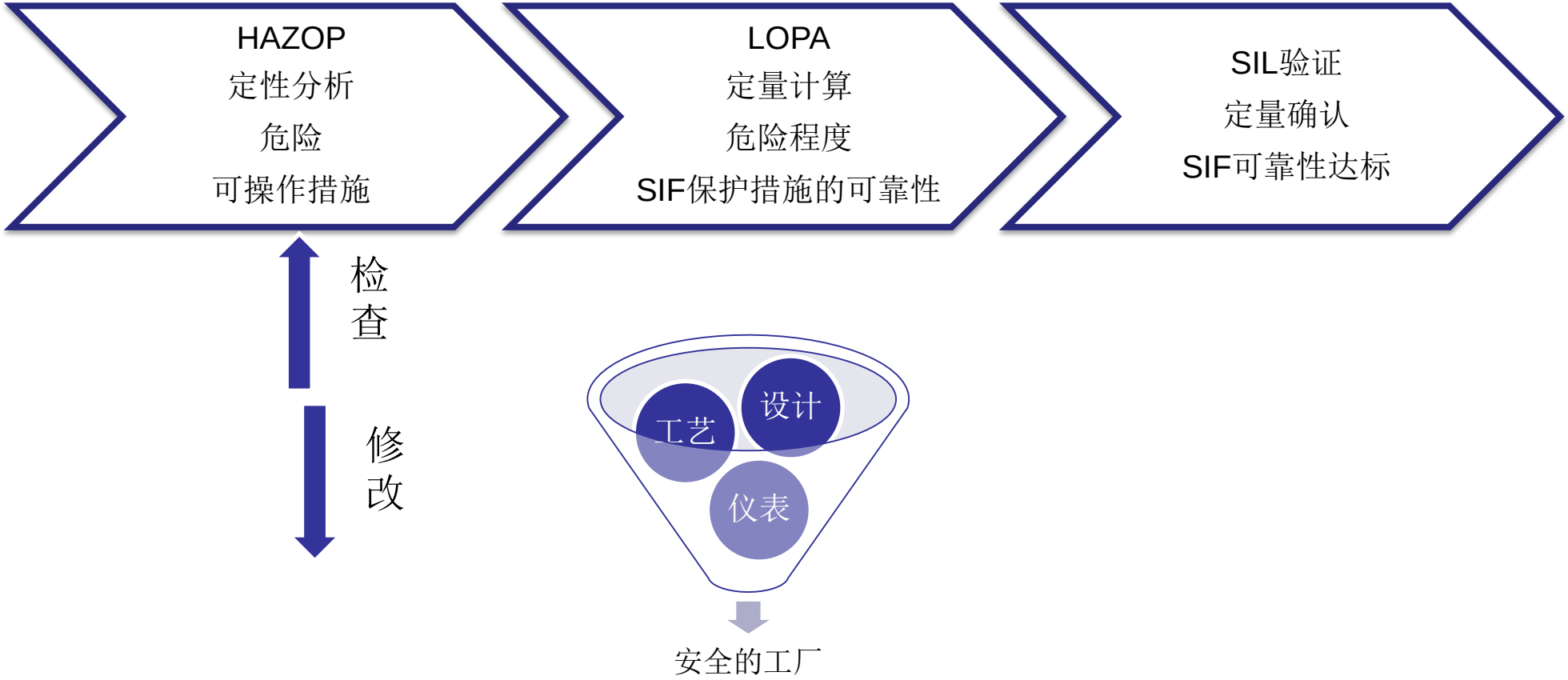
# 安全服务 Safety Service

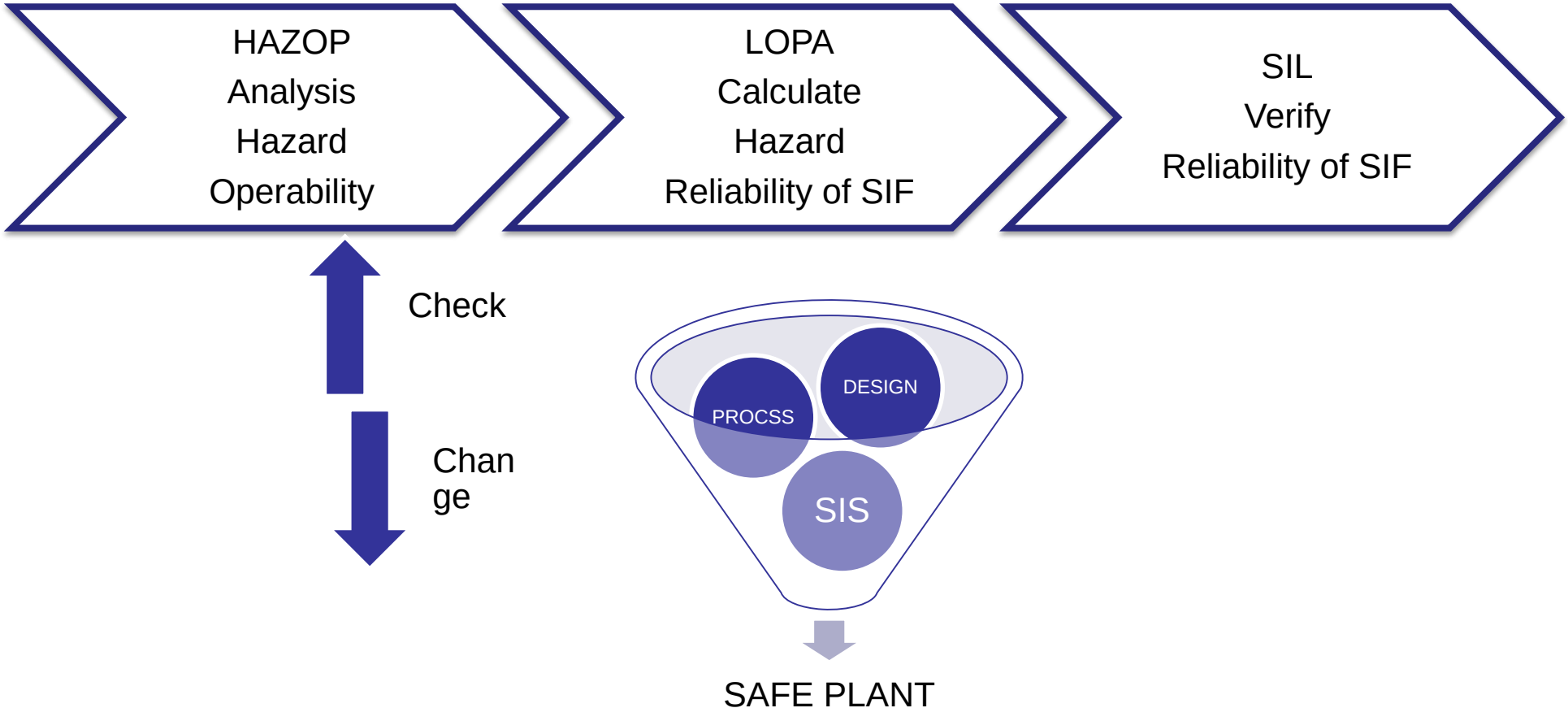
## SIL Hazop LOPA

阳上
YoungSun

# 安全服务


HAZOP
定性分析
危险
可操作措施
LOPA
定量计算
危险程度
SIF保护措施的可靠性
SIL验证
定量确认
SIF可靠性达标
检查
修改
工艺
设计
仪表
安全的工厂

# Safety Service



# 安全原理 SIS

量化危险

**建造安全**

风险后果严重程度
人员/财产/
环境/声誉

风险事故频率
经常/可能/偶尔/
极少/不可能

其他安全设施失效
安全阀
隔离措施

HAZOP
LOPA

需求

**SIL：SIS的可靠性**

SIL验证

实现

系统的结构

组件的可靠性

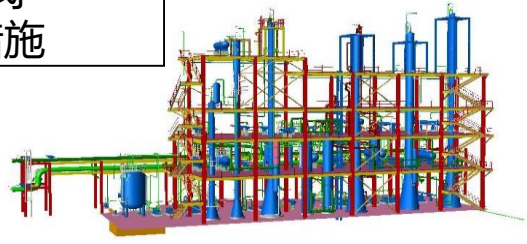
维护水平

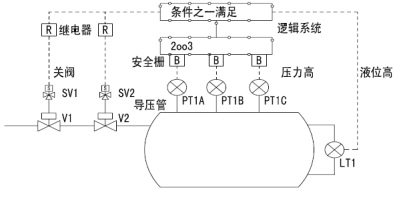
FMEA

实现

产品的设计

元件的可靠性





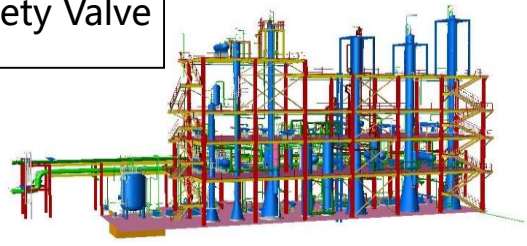

# Technology of Safety

Measure Dangerous

Consequence

Likelihood

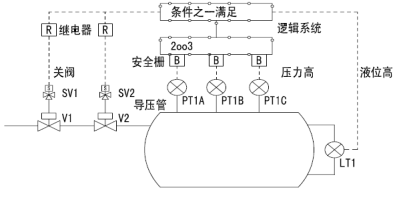
Other Protection Layers
Alarming, Safety Valve



HAZOP
LOPA

Requirement

**SIL：Reliability**




SIL
Verification

implement

**Build Safety**

Structure of System

Reliability of Instruments

Maintenance Leverage

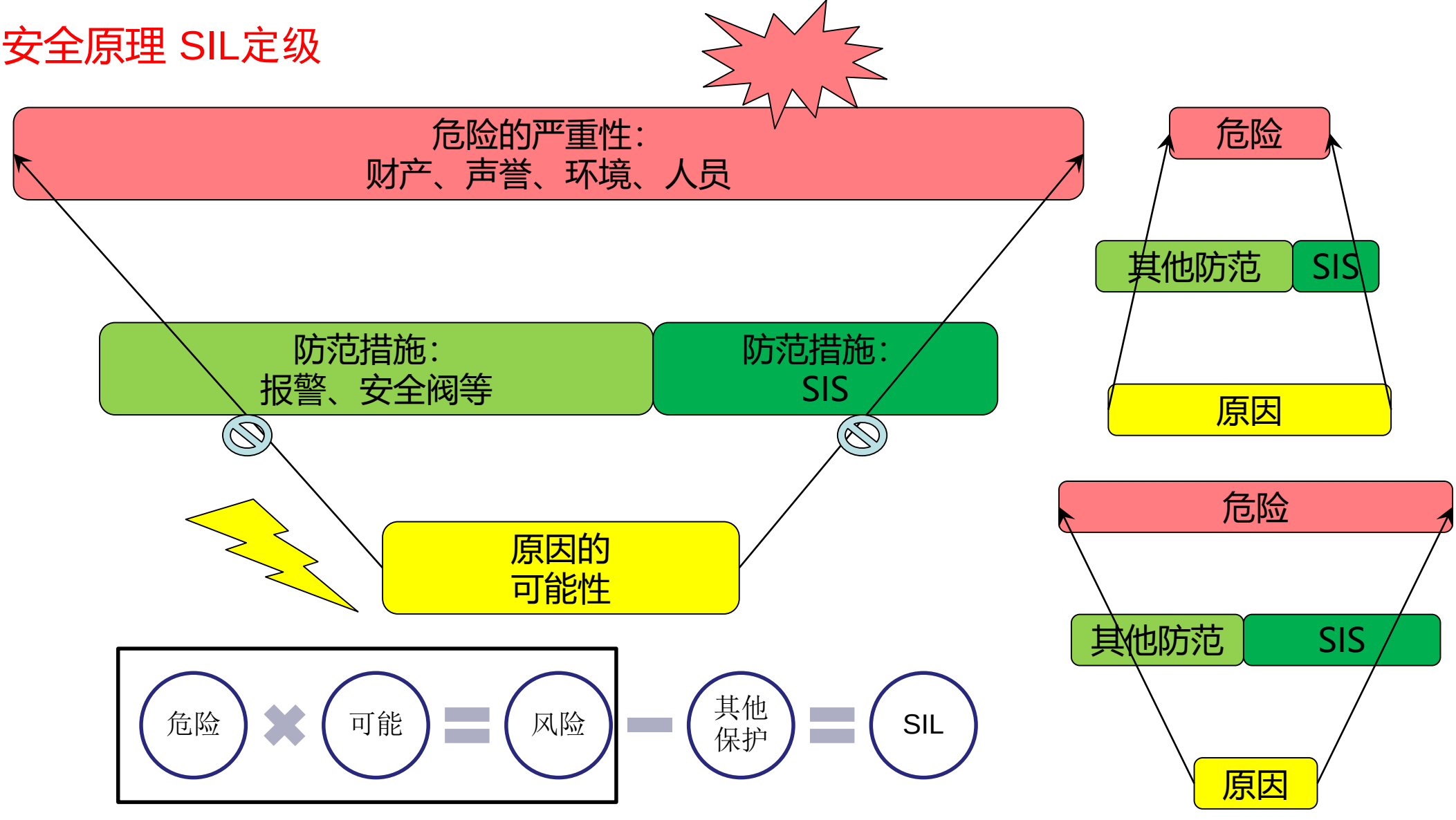
implement

FEMA

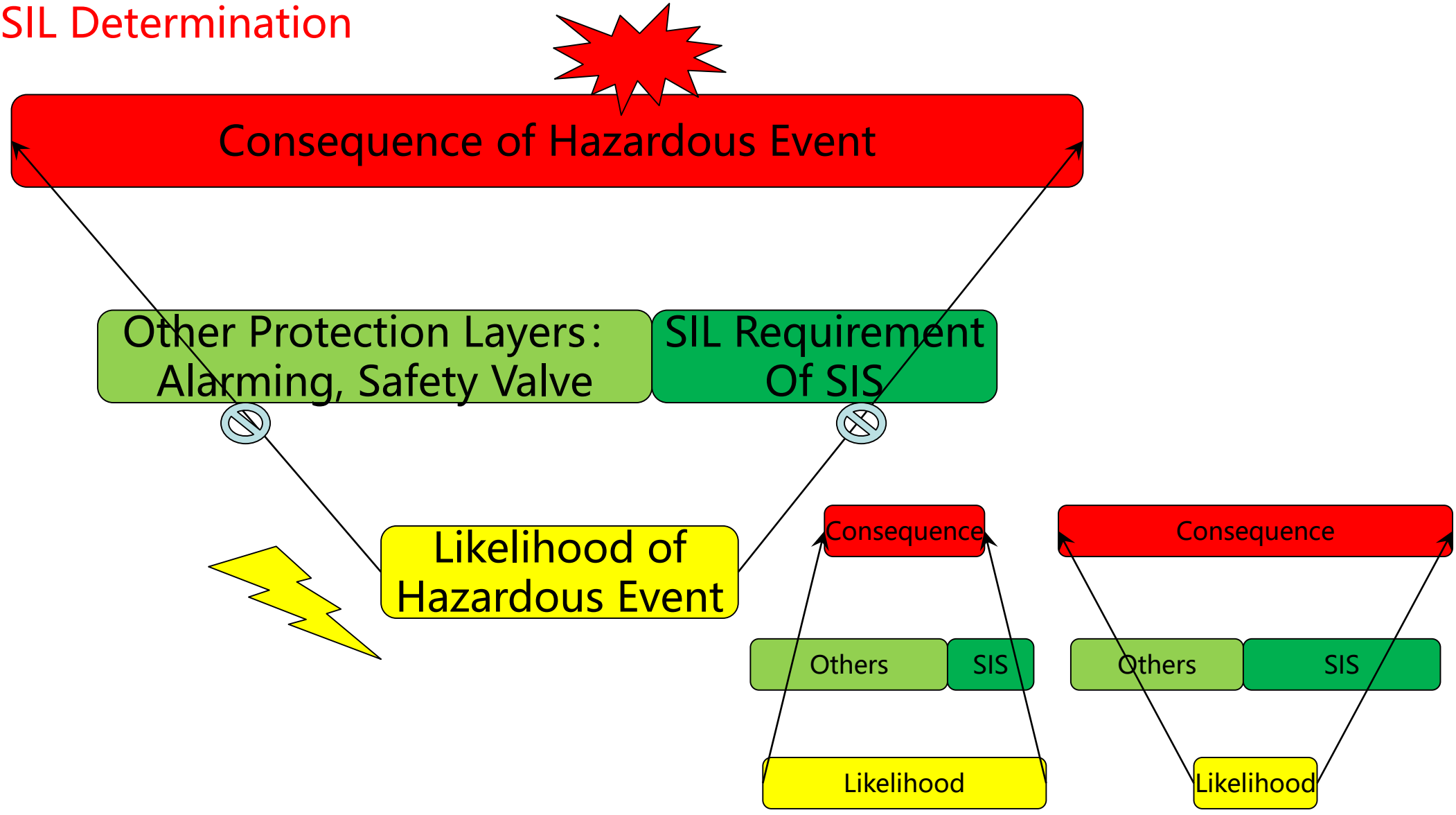
Design of Production

Reliability of Parts

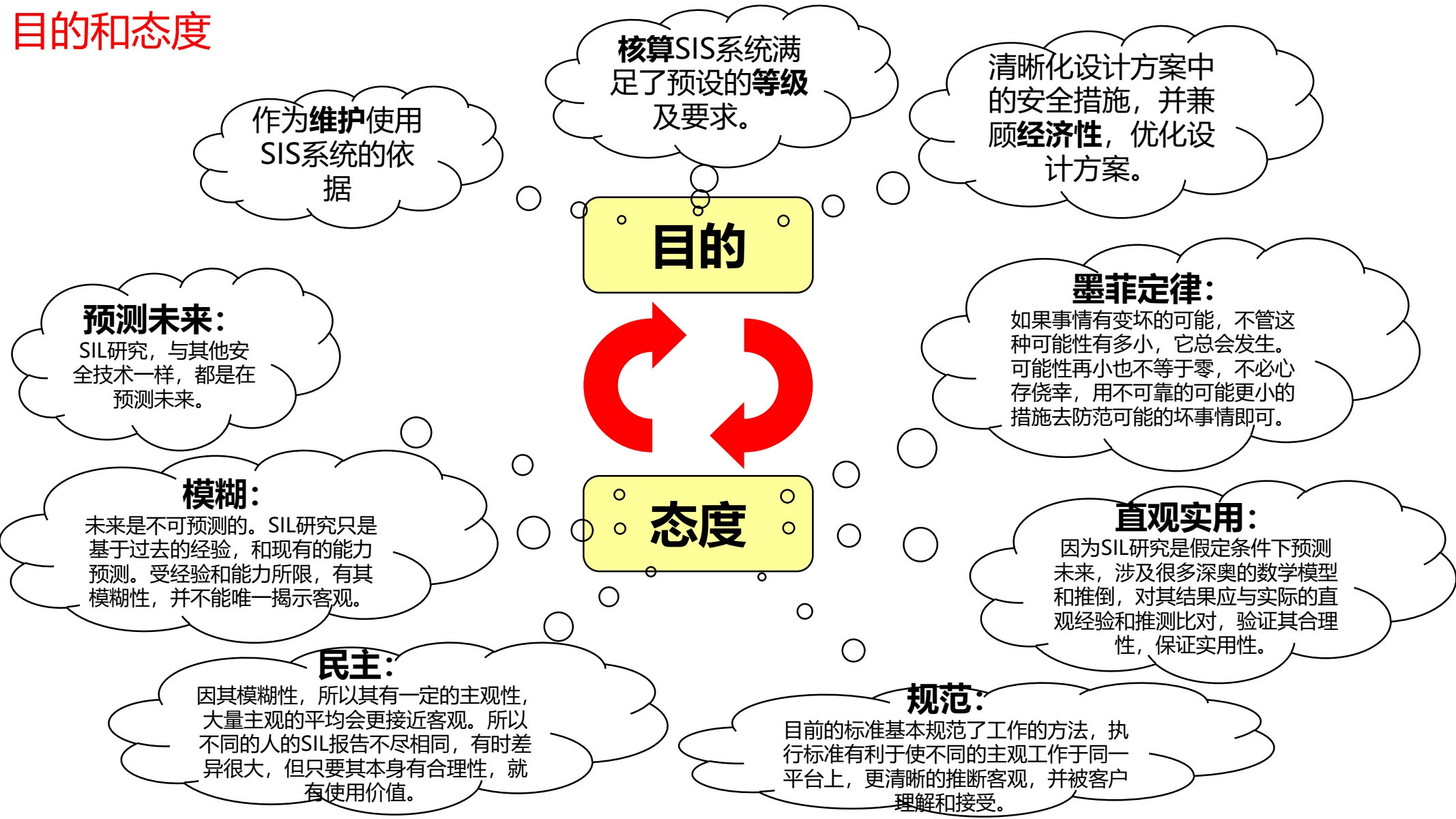
# 安全原理 SIL定级


危险的严重性：
财产、声誉、环境、人员
防范措施：
报警、安全阀等
防范措施：
SIS
原因的
可能性
危险
其他防范
SIS
原因
危险
其他防范
SIS
原因
危险
可能
风险
其他
保护
SIL

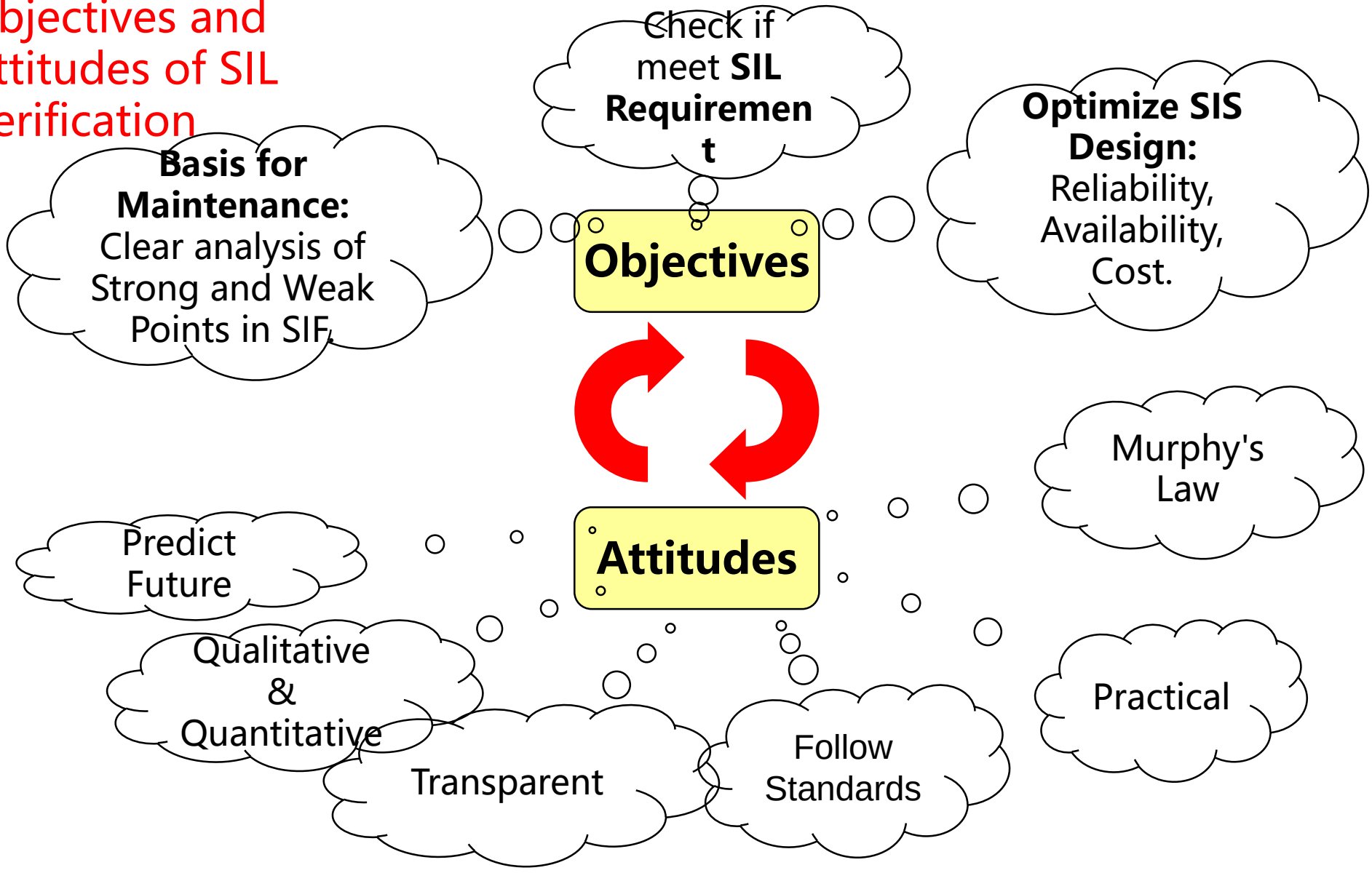
# SIL Determination



# 目的和态度

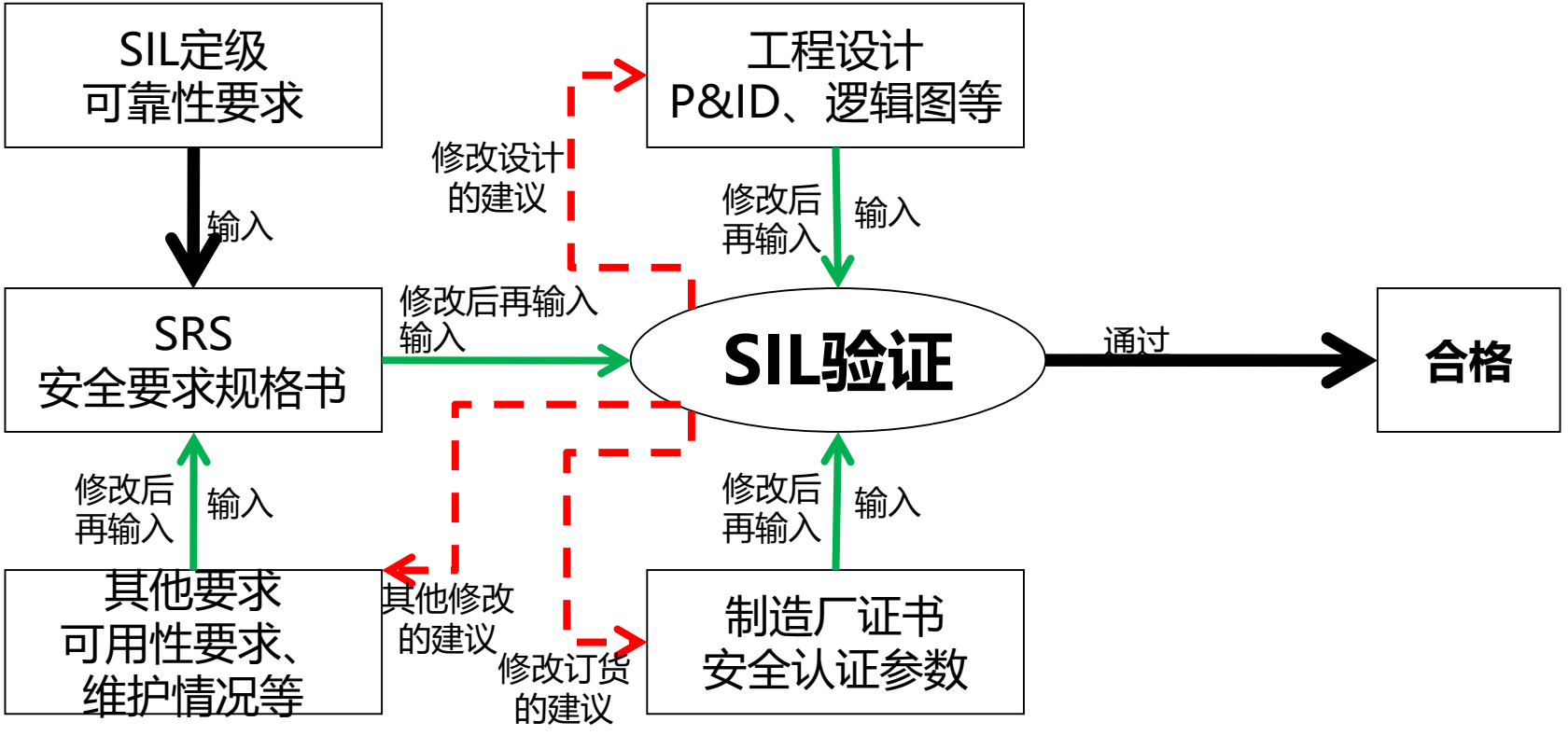

核算SIS系统满足了预设的等级及要求。
清晰化设计方案中的安全措施，并兼顾经济性，优化设计方案。
作为维护使用SIS系统的依据
目的
预测未来：
SIL研究，与其他安全技术一样，都是在预测未来。
墨菲定律：
如果事情有变坏的可能，不管这种可能性有多小，它总会发生。可能性再小也不等于零，不必心存侥幸，用不可靠的可能更小的措施去防范可能的坏事情即可。
模糊：
未来是不可预测的。SIL研究只是基于过去的经验，和现有的能力预测。受经验和能力所限，有其模糊性，并不能唯一揭示客观。
态度
直观实用：
因为SIL研究是假定条件下预测未来，涉及很多深奥的数学模型和推倒，对其结果应与实际的直观经验和推测比对，验证其合理性，保证实用性。
民主：
因其模糊性，所以其有一定的主观性，大量主观的平均会更接近客观。所以不同的人的SIL报告不尽相同，有时差异很大，但只要其本身有合理性，就有使用价值。
规范：
目前的标准基本规范了工作的方法，执行标准有利于使不同的主观工作于同一平台上，更清晰的推断客观，并被客户理解和接受。

# Objectives and Attitudes of SIL Verification



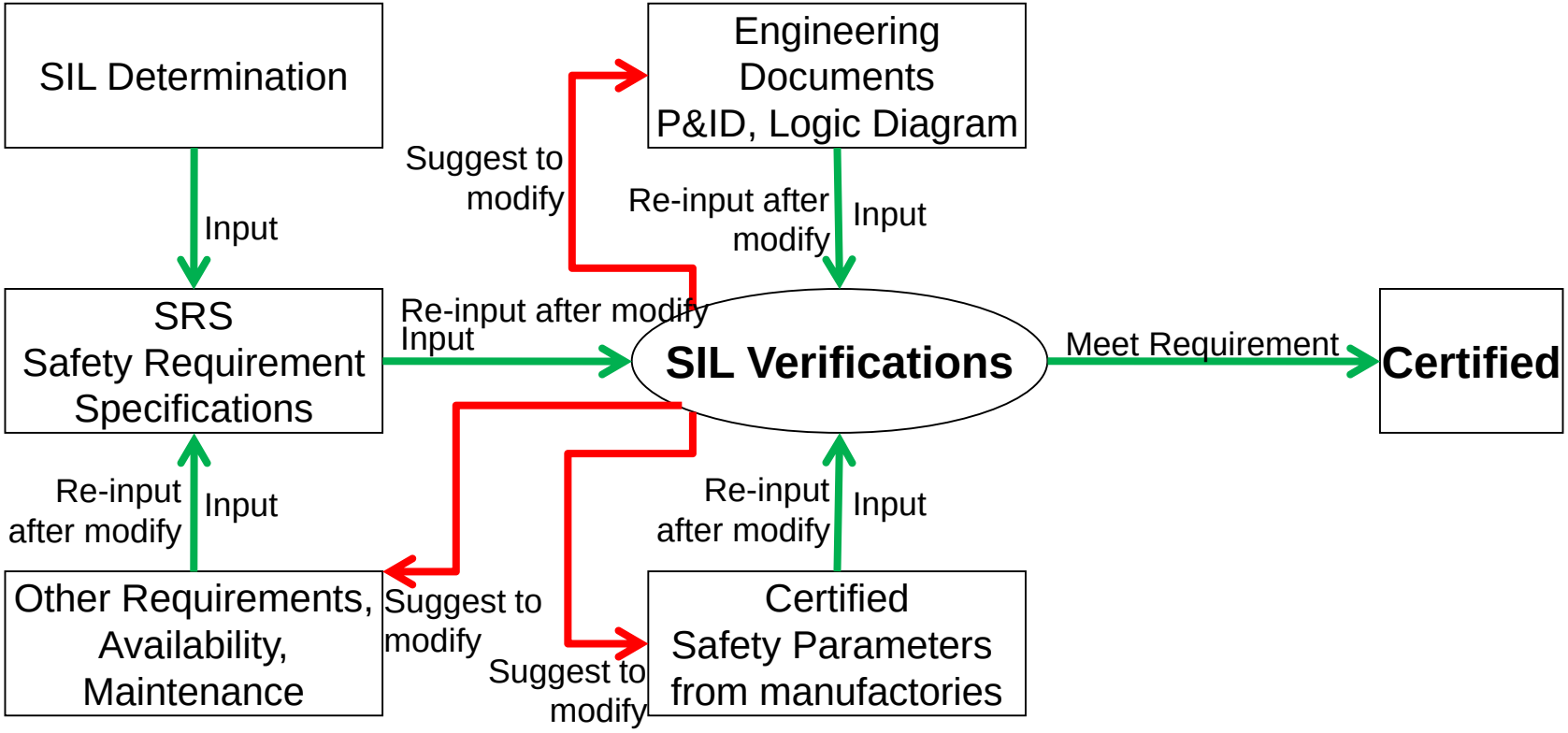
SIL验证 工作管理

SRS 工作管理



# Procedure of SIL Verification -1 : Outside





# SIL验证 计算原理

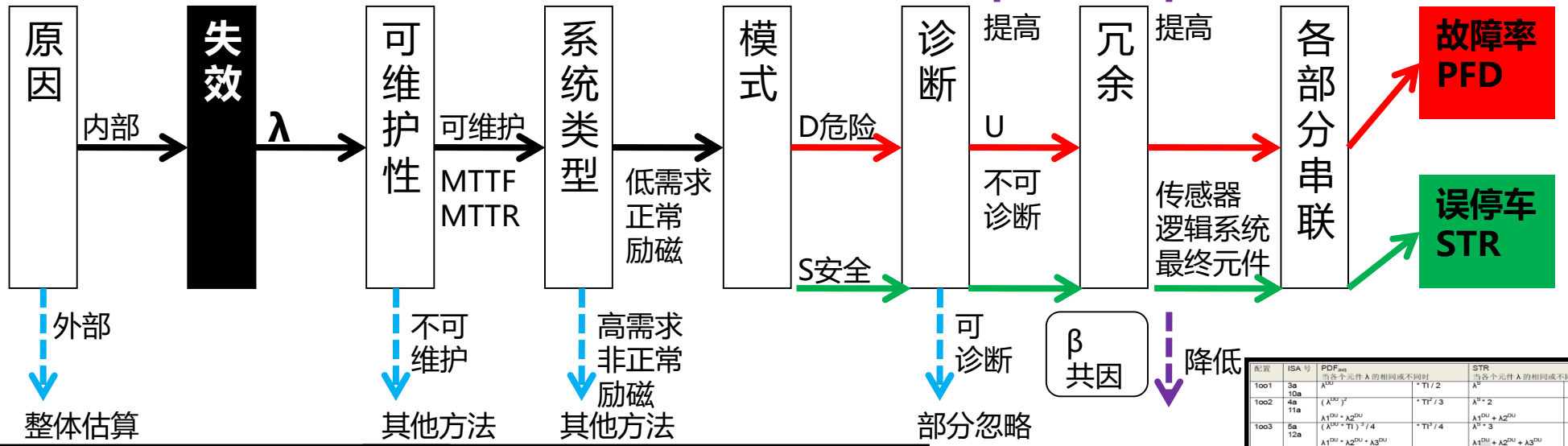
| | |
|---|---|
| PVST | Partial Valve Stoke Test<br>部分阀门行程测试<br>在工艺操作允许的情况下，通过定期对阀门<br>阀门各组件的故障，提高 DC，及时维修， |

| 配置 | $\lambda^{SD}$ | $\lambda^{SU}$ | $\lambda^{DD}$ | $\lambda^{DU}$ | $\lambda^{S}$ | $\lambda$ | DC |
|---|---|---|---|---|---|---|---|
| 无 PVST | | 165 | | 345 | 165 | 510 | 0 |
| 带 PVST | 165 | | 171 | 174 | 165 | 510 | 50% |
| 分析 | | | | | | | 提高了诊断 DC |
| | | | | | | | 总量没有变化 |
| | | | | | | | 没有影响安全故障 STR |
| | | | | | | | 降低了危险故障 PFD |
| | | | | | | | 诊断出部分的危险故障 |
| | | | | | | | 诊断出全部的安全故障 |

| 名称 | 定义 |
|---|---|
| TI | Test Interval 维护周期 |
| $PFD_{avg}$ | Average Probability of Failure on Demand 平均工作<br>在 TI 内，当需要时，系统或设备不能够完成某一特定<br>均值。<br>即：在维护周期内，工艺出现危险原因，但 SIS 不作 |
| FTA | Fault Tree Analysis 故障树分析<br>通过系统组件的故障的逻辑模型，估算系统故障的可 |

| SIL | 传感器和最终元件 | | 逻辑系统（依据其 SFF） | |
|---|---|---|---|---|
| | 基本要求 | 降级要 | | >90% |
| 1 | 0 | 0 | | 0 |
| 2 | 1 | 0 | | 0 |
| 3 | 2 | 1 | | 1 |

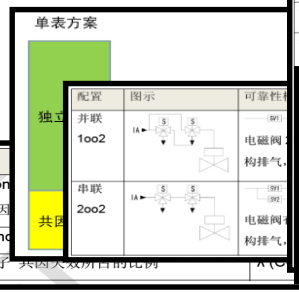
| SIL | PDFavg |
|---|---|
| 1 | < 1 / 10 |
| 2 | < 1 / 100 |
| 3 | < 1 / 1000 |




| λ<br>失效 | U Undetected<br>不可检测的 | D Detected<br>可检测的 |
|---|---|---|
| D<br>Dangerous<br>危险失效 | 例如：<br>失效源：电磁阀机械卡死，需要失电放气时不能按需求工作。<br>SIS 状态：失效状态。此时如果变送器测量到压力超限，需要停车却做不到。<br>工艺状态：处于无保护的状态。 | 例如：<br>失效源：热电偶被烧穿，但是温变检测了出来，报警。<br>SIS 状态：可以及时维护。<br>工艺状态：并不至于处于类似“电磁阀机械卡死”的无保护状态；但是，有可能会类似“电磁阀线圈烧断”产生误停车。 |
| S<br>Safety<br>安全失效 | 例如：<br>失效源：电磁阀线圈断了<br>SIS 状态：电磁阀失电动作<br>工艺状态：虽然没有工艺故障，但是误停车，将工艺流程切换到安全的状态。 | |

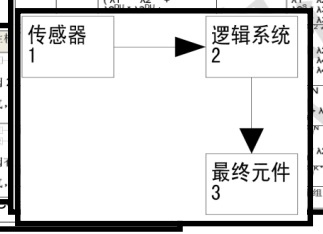

| 名称 | 定义 | 举例 |
|---|---|---|
| 正常励磁 | 无需求时，<br>SIS 处于励磁的状态。 | 工艺正常，电磁阀<br>工艺故障，电磁阀 |
| 非正常励磁<br>即：故障安全型 | 无需求时，<br>SIS 处于非励磁的状态。 | 工艺正常，电磁阀<br>工艺故障，电磁阀 |

| 名称 | 定义 |
|---|---|
| CCF | Common<br>共同原因 |
| IF | Independ |
| β | 共因因子 |

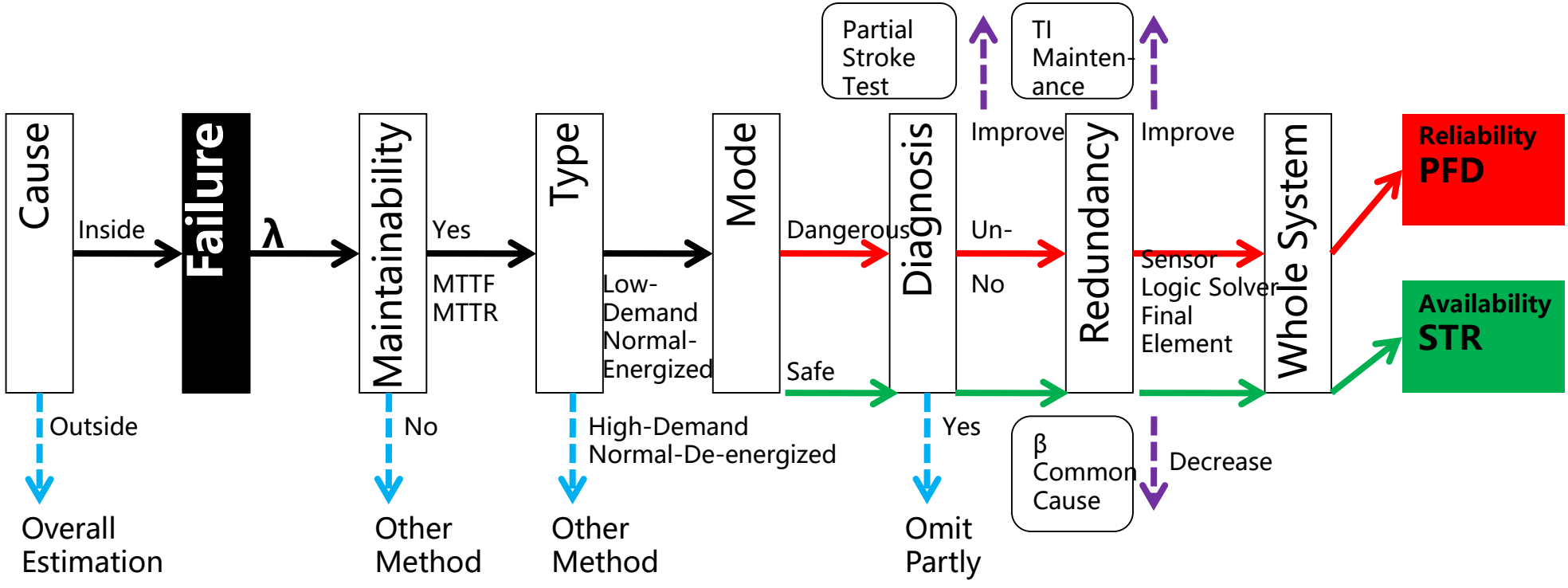



| 配置 | 图示 | 可靠性 |
|---|---|---|
| 并联<br>1oo2 | | 电磁阀<br>构排气 |
| 串联<br>2oo2 | | 电磁阀<br>构排气 |

| 配置 | ISA 号 | $PDF_{avg}$<br>当各个元件 λ 的相同或不同时 | | STR<br>当各个元件 λ 的相同或不同时 | |
|---|---|---|---|---|---|
| 1oo1 | 3a<br>10a | $\lambda^{DU}$ | * TI / 2 | $\lambda^{S}$ | |
| 1oo2 | 4a<br>11a | $(\lambda^{DU})^2$<br>$\lambda 1^{DU} * \lambda 2^{DU}$ | * TI / 3 | $\lambda^{S} * 2$<br>$\lambda 1^{DU} + \lambda 2^{DU}$ | |
| 1oo3 | 5a<br>12a | $(\lambda^{DU} * TI)^3 / 4$<br>$\lambda 1^{DU} * \lambda 2^{DU} * \lambda 3^{DU}$ | * TI² / 4 | $\lambda^{S} * 3$<br>$\lambda 1^{DU} * \lambda 2^{DU} + \lambda 3^{DU}$ | |
| 2oo2 | 6a<br>13a | $\lambda^{DD}$<br>$(\lambda 1^{DU} + \lambda 2^{DU}) / 2$ | * TI | $(\lambda^{S})^2$<br>$\lambda 1^{DU} * \lambda 2^{DU}$ | *2*MTTR |
| 2oo3 | 7a<br>14a | $(\lambda^{DU})^2 * 3$<br>$(\lambda 1^{DU} * \lambda 2^{DU} +$ | * TI² | $(\lambda^{S})^2 * 3$<br>$\lambda 1^{S} * \lambda 2^{S} +$ | *2* MTTR |
| | | | | $\lambda 1^{S} * \lambda 3^{S} +$ | |
| | | | | $\lambda 2^{S} * \lambda 3^{S} +$ | |
| | | | | $\lambda 1^{S} * \lambda 2^{S} * \lambda 3^{S}$ | *2*MTTR |
| | | | | $\lambda 2^{S} + \lambda 1^{S} * \lambda 3^{S} +$ | |
| | | | | $\lambda 4^{S} + \lambda 2^{S} * \lambda 3^{S} +$ | |
| | | | | $\lambda 4^{S} + \lambda 3^{S} * \lambda 4^{S} +$ | |
| | | | | $\lambda 2^{S} + \ldots +$ | |
| | | | | $\lambda 2^{S} + \ldots *$ | * 1*2*…*N<br>*(MTTR)^(N-1) |
| | | | | $C_N^K$ | *$P_K$<br>*(MTTR)^(K-1) |

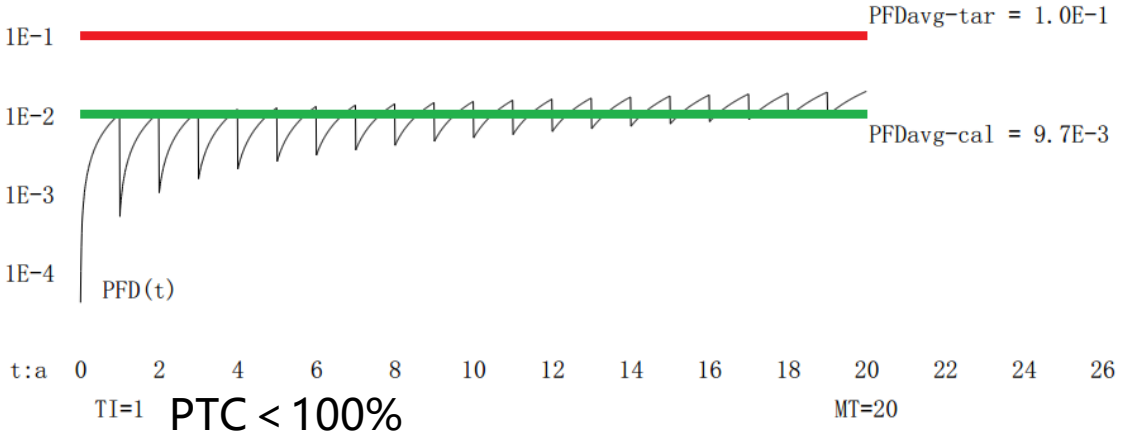


# Procedure of SIL Verification -2 : Inside



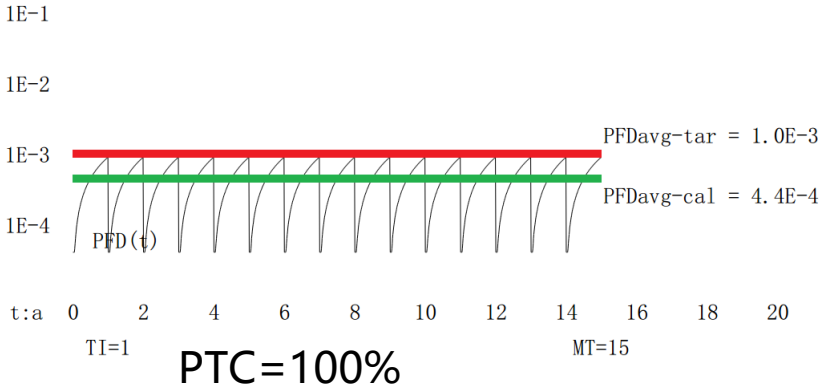
# SIL验证 系统 参数 MT/PTC

## SRS 数据 维护

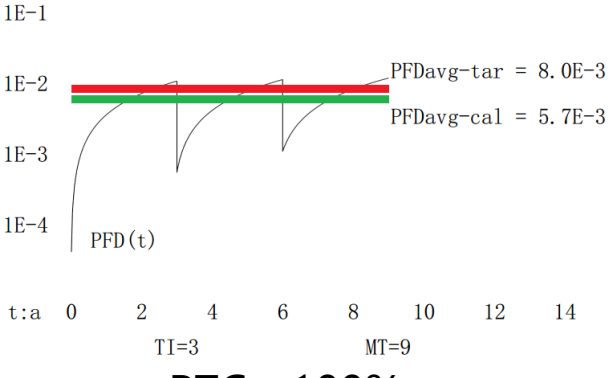



PTC < 100%

PTC < 100%:
PFDavg(TI) 提高至 PFDavg(MT)。
PTC=100%:
PFDavg(TI) = PFDavg(MT)。



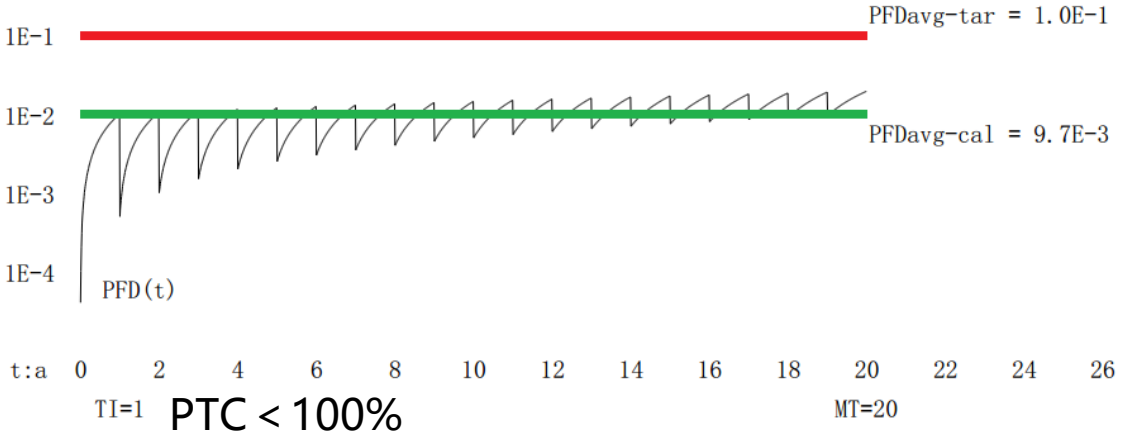

PTC=100%




PTC < 100%

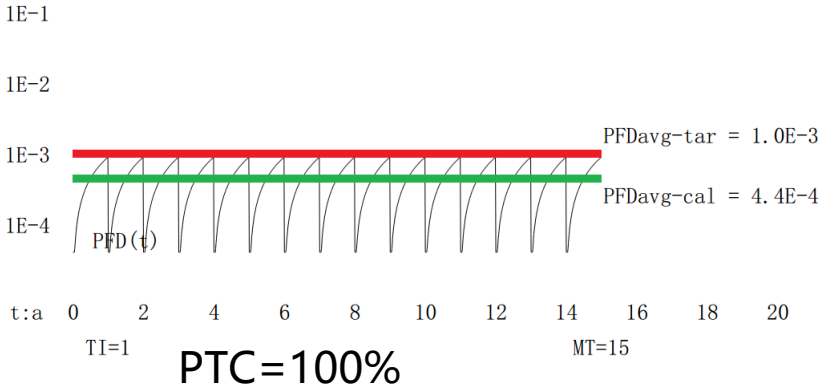
# SIL Verification MT/PTC

# SRS Data

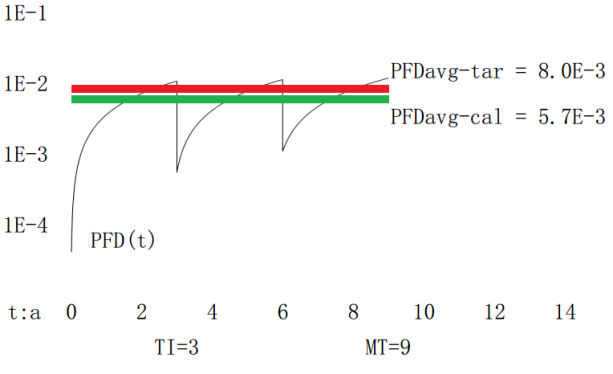



PTC < 100%

PTC < 100%:
PFDavg(TI) Increase to PFDavg(MT).
PTC=100%:
PFDavg(TI) = PFDavg(MT).

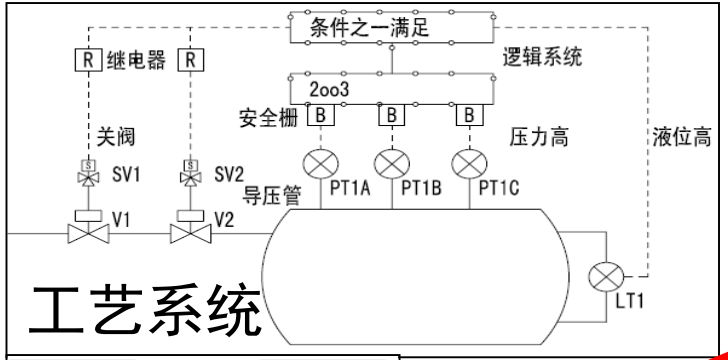


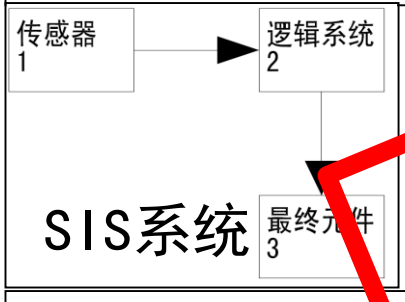

PTC=100%



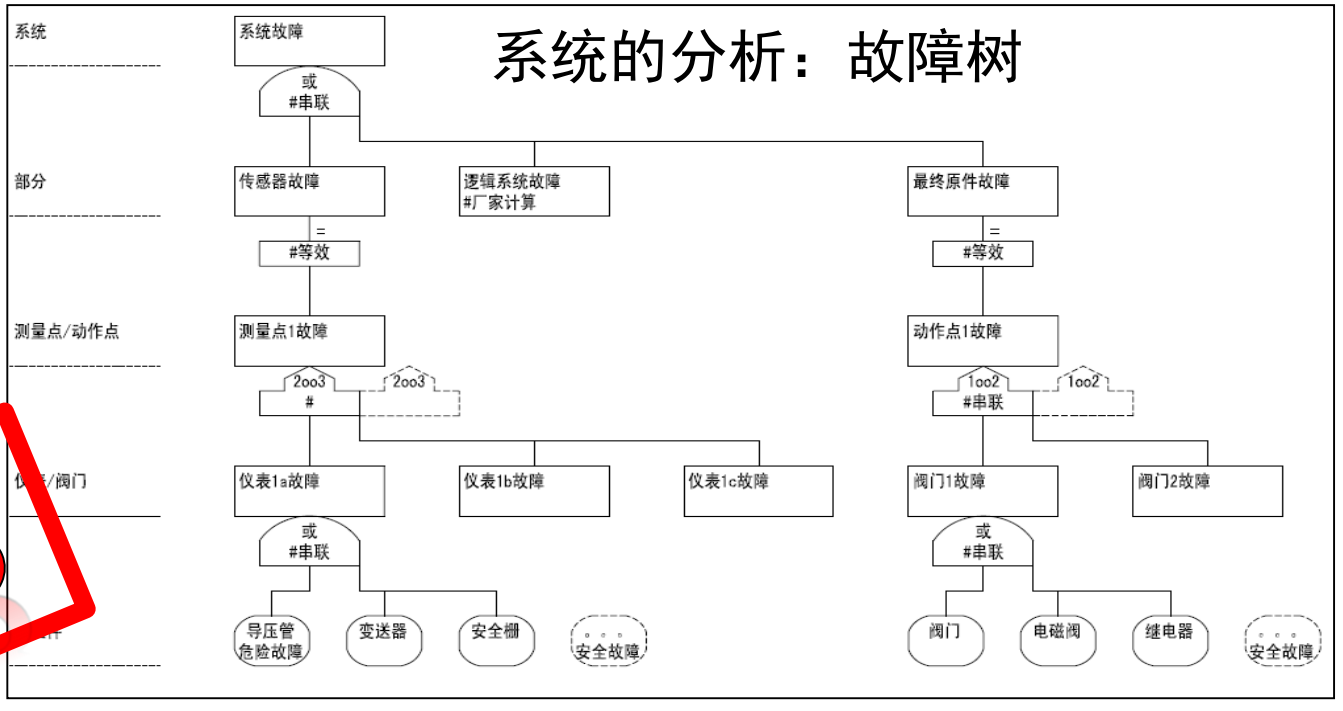

PTC < 100%

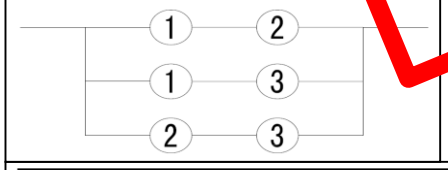
# SIL验证 系统 计算




SIL3



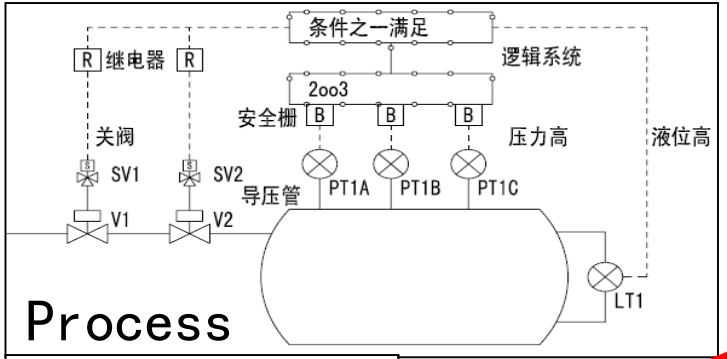



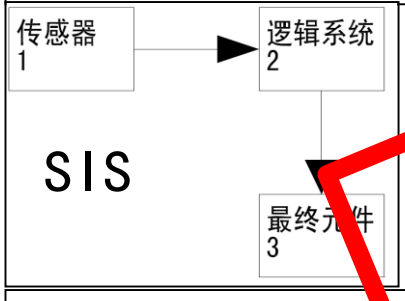

环节的分析：2oo3的可靠路径

系统的分析：计算

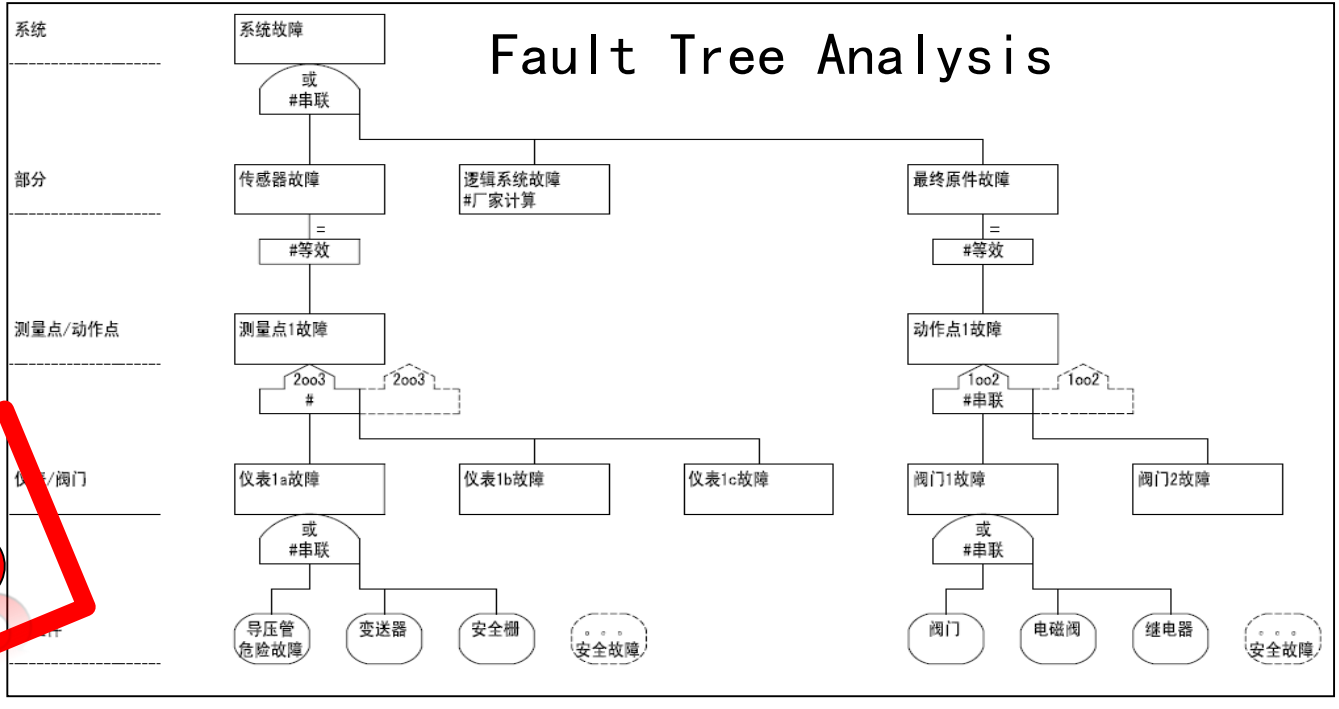
| 部分 | 各部分分计 PFD | 各部分分计 STR | 占比 PFD | 占比 STR | 配置 | 测量点 动作点 | 共因调整后 PFD | 共因调整后 STR | 配置 | 估值 β | 估值 MTTR | 仪表位号 | 配置 | 组成名称 | 制造厂 | 型号 | 规格 | 应用 | λDU | λS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 传感器 | 0.02 | 0.01 | 0% | 0% | | | | | | | | | | | | | | | | |
| | | | | | | 压力测量 | 0.02 | 0.01 | 2oo3 | 2% | 4 | | | | | | | | | |
| | | | | | | | | | | | | PT1a | 同下 | | | | | | | |
| | | | | | | | | | | | | PT1b | 串联 | | | | | | | |
| | | | | | | | | | | | | | | 导压管 | | | | 干净 | 50 | 50 |
| | | | | | | | | | | | | | | 压力变送器 | Emerson | 3051 | | | 50 | 100 |
| | | | | | | | | | | | | | | 安全栅 | 通用 | | | | 50 | 150 |

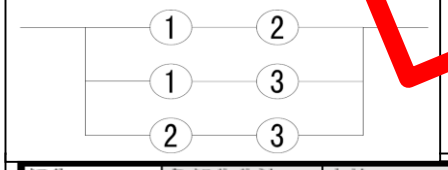
# SIL Verification Calculate




SIL3




## Reliability Analysis

## Calculate

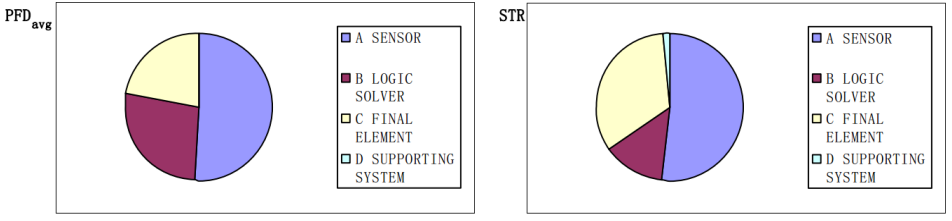
| 部分 | 各部分分计 PFD | 各部分分计 STR | 占比 PFD | 占比 STR | 配置 | 测量点 动作点 | 共因调整后 PFD | 共因调整后 STR | 配置 | 估值 β | 估值 MTTR | 仪表位号 | 配置 | 组成名称 | 制造厂 | 型号 | 规格 | 应用 | λDU | λS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 传感器 | 0.02 | 0.01 | 0% | 0% | | | | | | | | | | | | | | | | |
| | | | | | | 压力测量 | 0.02 | 0.01 | 2oo3 | 2% | 4 | | | | | | | | | |
| | | | | | | | | | | | | PT1a | 同下 | | | | | | | |
| | | | | | | | | | | | | PT1b | 串联 | | | | | | | |
| | | | | | | | | | | | | | | 导压管 | | | | 干净 | 50 | 50 |
| | | | | | | | | | | | | | | 压力变送器 | Emerson | 3051 | | | 50 | 100 |
| | | | | | | | | | | | | | | 安全栅 | 通用 | | | | 50 | 150 |

# SIL验证 系统 计算 例子

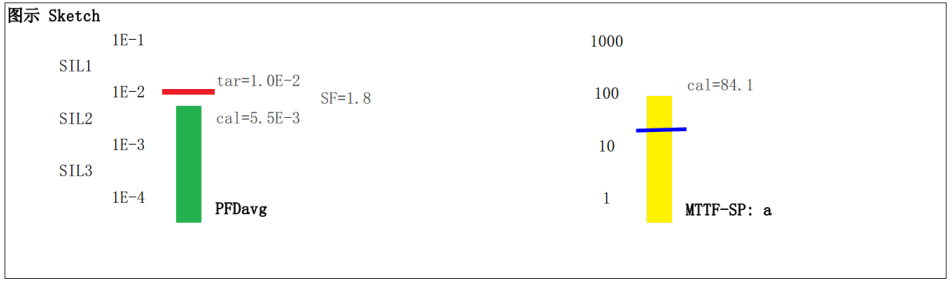
**结果 Result**

| | 目标 Target | 说明 Notes | 实现 Arch. | 说明 Notes | 检查 Check |
|---|---|---|---|---|---|
| SIL | 2 | 低需求 LowDemand. | | | 通过 Pass |
| PFDavg | 1.0E-02 | 1.0E-03 ~ 1.0E-02 | 5.5E-03 | | 满足 Meet |
| MTTF-SP | | a | 84.1 | STR=1.4E-06 | 满足 Meet |
| HFT | 0 | 按照GB/T 21109 Follow IEC 61511 | 0 | | 满足 Meet |
| SC | 2 | | 3 | | 满足 Meet |

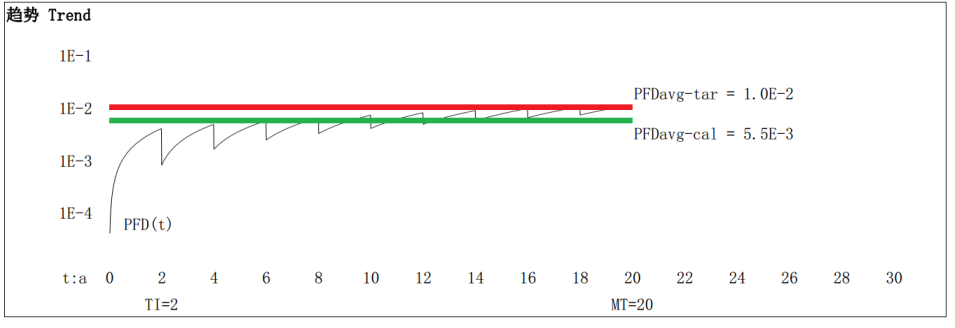
**分布 Split**

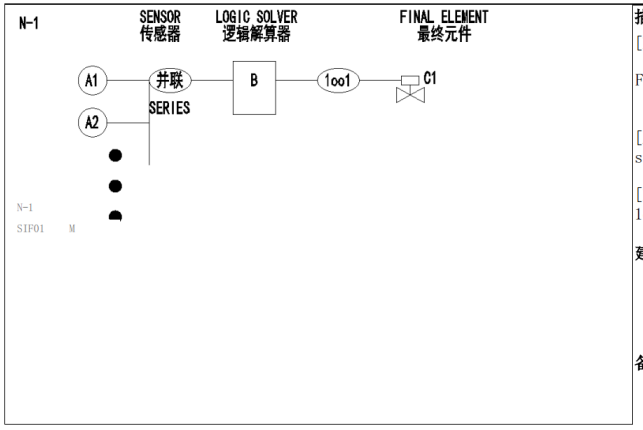



**图示 Sketch**




**趋势 Trend**




**描述 Description**

[PID]

Flowmeter at vent pipe of ---

[Action] FIQ not reach
set pointclose inlet valve
in SIS.
[Remark] In SIS,Sensor: 1oo1,FE: 1oo1 [System] SIS

**建议 Suggestion**

**备注 Remark**

**输入 Input** λ : FIT (E-9/h)

| 位号Tag | PTC | λ DU | λ SP | 配置Conf. | 组件描述Description | SC | Type | λ SP | DC | SFF | λ DU | λ DD | λ SU | λ SD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FT | 80% | 170 | 180 | Series | Vortex Flowmeter E+H 7F2C15 Refer General | 2 | B | 180 | 0% | 51% | 170 | 0 | 180 | 0 |
| LS | 80% | 7 | 22 | Series | Proximity Switch P+F NJ2-12GM-N-5M | 3 | A | 22 | 0% | 76% | 7 | 0 | 22 | 0 |
| SIS | 80% | 41 | 124 | Series | Barrier P&F KFD2-SR2-EX1.W Discrete | 3 | A | 113 | 0% | 75% | 38 | 0 | 113 | 0 |
| | | | | | DI Siemens 6ES7 136-6AA00-0CA1 | 3 | B | 9 | 0% | 80% | 2 | 0 | 9 | 0 |
| | | | | | Controller Siemens S7-1500 | 3 | B | 1 | 0% | 82% | 0 | 0 | 1 | 0 |
| | | | | | DO Siemens 6ES7 136-6DB00-0CA0 | 3 | B | 1 | 0% | 82% | 0 | 0 | 1 | 0 |
| V | 80% | 46 | 179 | Series | Valve Kingdom KV-L6G-A Ball valve FC, Refer General | 3 | A | 2 | 25% | 25% | 6 | 2 | 0 | 0 |
| | | | | | Actuator Air Torque ATx01US10 Single acting | 3 | A | 0 | 0% | 0% | 10 | 0 | 0 | 0 |
| | | | | | Solenoid Norgren #971051546020240 DE | 3 | A | 177 | 0% | 86% | 30 | 0 | 177 | 0 |

**子系统 Sub-system**

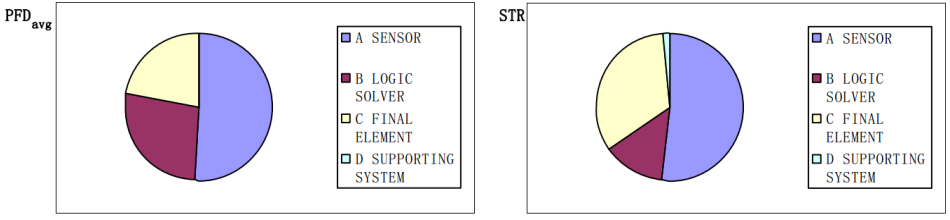
| 子系统Sub. | PFDavg | 占比 % | STR | 占比 % | HFT | 配置Conf. | 部分Part | PFDavg | STR | 配置Conf. | β | TI:a | MT:a | MTTR:h |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SENSOR | 4.3E-03 | 67% | 2.0E-07 | 38% | 0 | Series | Sensor 1 | 4.2E-03 | 1.8E-07 | 1oo1 | | 2 | 20 | |
| | | | | | | | Sensor 1 | 1.7E-04 | 2.2E-08 | 1oo1 | | 2 | 20 | |
| LOGIC SOLVER | 1.0E-03 | 15% | 1.2E-07 | 24% | 1 | | SIS | 1.0E-03 | 1.2E-07 | 1oo1 | | 2 | 20 | |
| FINAL ELEMENT | 1.1E-03 | 17% | 1.8E-07 | 34% | 0 | 1oo1 | Valve 1 | 1.1E-03 | 1.8E-07 | 1oo1 | | 2 | 20 | |
| SUPPORTING SYSTEM | | | 2.0E-08 | 4% | | | | | | | | | | |

# SIL Verification Sample

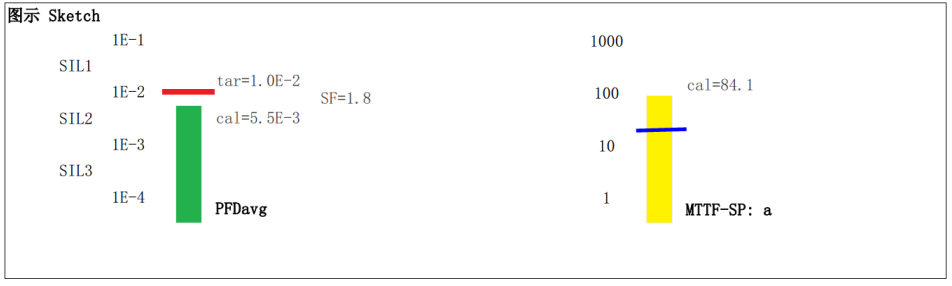
**结果 Result**

| | 目标 Target | 说明 Notes | 实现 Arch. | 说明 Notes | 检查 Check |
|---|---|---|---|---|---|
| SIL | 2 | 低需求 LowDemand. | | | 通过 Pass |
| PFDavg | 1.0E-02 | 1.0E-03 ~ 1.0E-02 | 5.5E-03 | | 满足 Meet |
| MTTF-SP | | a | 84.1 | STR=1.4E-06 | 满足 Meet |
| HFT | 0 | 按照GB/T 21109 Follow IEC 61511 | 0 | | 满足 Meet |
| SC | 2 | | 3 | | 满足 Meet |

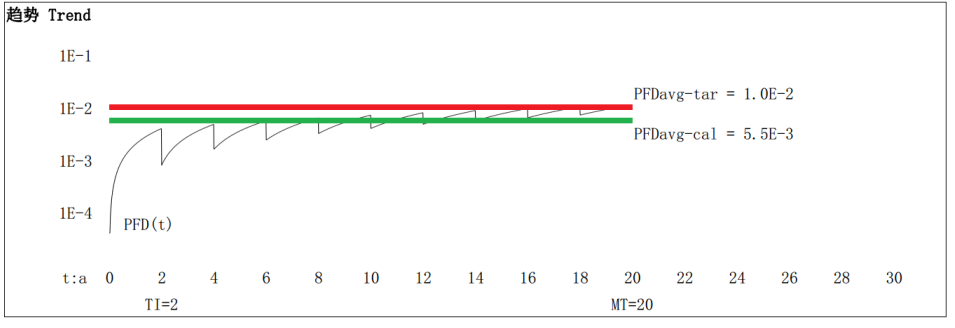
**分布 Split**

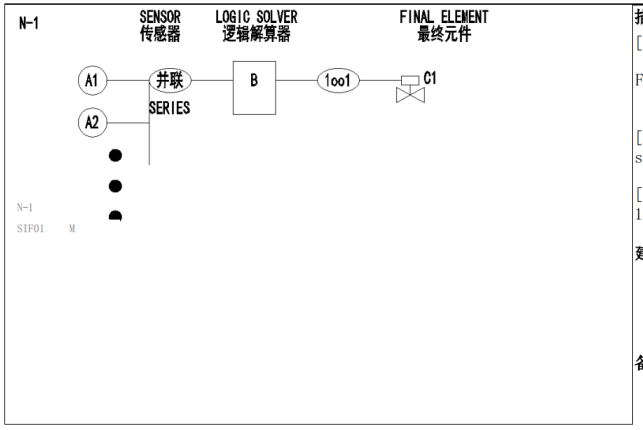



**图示 Sketch**




**趋势 Trend**




**描述 Description**

[PID]

Flowmeter at vent pipe of ---

[Action] FIQ not reach
set pointclose inlet valve
in SIS.
[Remark] In SIS,Sensor: 1oo1,FE: 1oo1 [System] SIS

**建议 Suggestion**

**备注 Remark**

**输入 Input** λ : FIT (E-9/h)

| 位号Tag | PTC | λ DU | λ SP | 配置Conf. | 组件描述Description | SC | Type | λ SP | DC | SFF | λ DU | λ DD | λ SU | λ SD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FT | 80% | 170 | 180 | Series | Vortex Flowmeter E+H 7F2C15 Refer General | 2 | B | 180 | 0% | 51% | 170 | 0 | 180 | 0 |
| LS | 80% | 7 | 22 | Series | Proximity Switch P+F NJ2-12GM-N-5M | 3 | A | 22 | 0% | 76% | 7 | 0 | 22 | 0 |
| SIS | 80% | 41 | 124 | Series | Barrier P&F KFD2-SR2-EX1.W Discrete | 3 | A | 113 | 0% | 75% | 38 | 0 | 113 | 0 |
| | | | | | DI Siemens 6ES7 136-6AA00-0CA1 | 3 | B | 9 | 0% | 80% | 2 | 0 | 9 | 0 |
| | | | | | Controller Siemens S7-1500 | 3 | B | 1 | 0% | 82% | 0 | 0 | 1 | 0 |
| | | | | | DO Siemens 6ES7 136-6DB00-0CA0 | 3 | B | 1 | 0% | 82% | 0 | 0 | 1 | 0 |
| V | 80% | 46 | 179 | Series | Valve Kingdom KV-L6G-A Ball valve FC, Refer General | 3 | A | 2 | 25% | 25% | 6 | 2 | 0 | 0 |
| | | | | | Actuator Air Torque ATx01US10 Single acting | 3 | A | 0 | 0% | 0% | 10 | 0 | 0 | 0 |
| | | | | | Solenoid Norgren #971051546020240 DE | 3 | A | 177 | 0% | 86% | 30 | 0 | 177 | 0 |

**子系统 Sub-system**

| 子系统Sub. | PFDavg | 占比 % | STR | 占比 % | HFT | 配置Conf. | 部分Part | PFDavg | STR | 配置Conf. | β | TI:a | MT:a | MTTR:h |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SENSOR | 4.3E-03 | 67% | 2.0E-07 | 38% | 0 | Series | Sensor 1 | 4.2E-03 | 1.8E-07 | 1oo1 | | 2 | 20 | |
| | | | | | | | Sensor 1 | 1.7E-04 | 2.2E-08 | 1oo1 | | 2 | 20 | |
| LOGIC SOLVER | 1.0E-03 | 15% | 1.2E-07 | 24% | 1 | | SIS | 1.0E-03 | 1.2E-07 | 1oo1 | | 2 | 20 | |
| FINAL ELEMENT | 1.1E-03 | 17% | 1.8E-07 | 34% | 0 | 1oo1 | Valve 1 | 1.1E-03 | 1.8E-07 | 1oo1 | | 2 | 20 | |
| SUPPORTING SYSTEM | | | 2.0E-08 | 4% | | | | | | | | | | |

阳上
YoungSun

0086-13911716191
Young66666@163.com