课件3：安全仪表系统SIS设计与工程

- 声明：本课件非本公司编制，来源于网络.

青岛劳帕安全技术咨询有限公司

核心业务

- 安全仪表系统功能评估：安全完整性等级SIL定级、验证/验算
- 过程工艺危害分析 **HAZOP**
- 培训：安全完整性等级SIL定级、验证/验算、HAZOP等培训

微信扫一扫

微信号 :**qd13184148810**

电话：13184148810

QQ:1930712371

邮箱：qingdaolopa@163.com

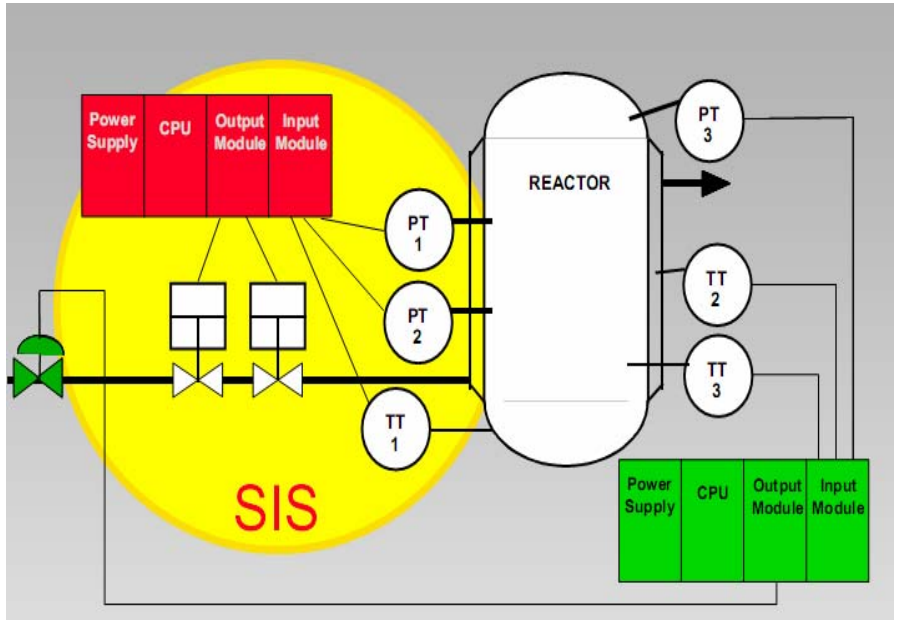
网址：www.qingdaolopa.com

目的

目的

设计一个或多个SIS，以提供安全仪表的功能，并满足规定的安全完整性等级。

SIS特征:
- 高可靠性
- 避免失效
- 无法避免时,失效要以可预见的方式出现



BPCS

安全仪表功能(SIF)

- safety instrumented Function
- 具有某个特定的SIL，用以达到功能安全的安全功能，它既可以是一个仪表安全保护功能，也可以是一个仪表安全控制功能。
- 安全仪表功能的描述包括两部分：
  - 安全功能要求（功能用来做什么）
  - 安全完整性要求（安全功能按要求执行的可靠性）
- 安全功能要求是由风险分析确定的，安全完整性要求由风险评估中得出。

安全仪表功能

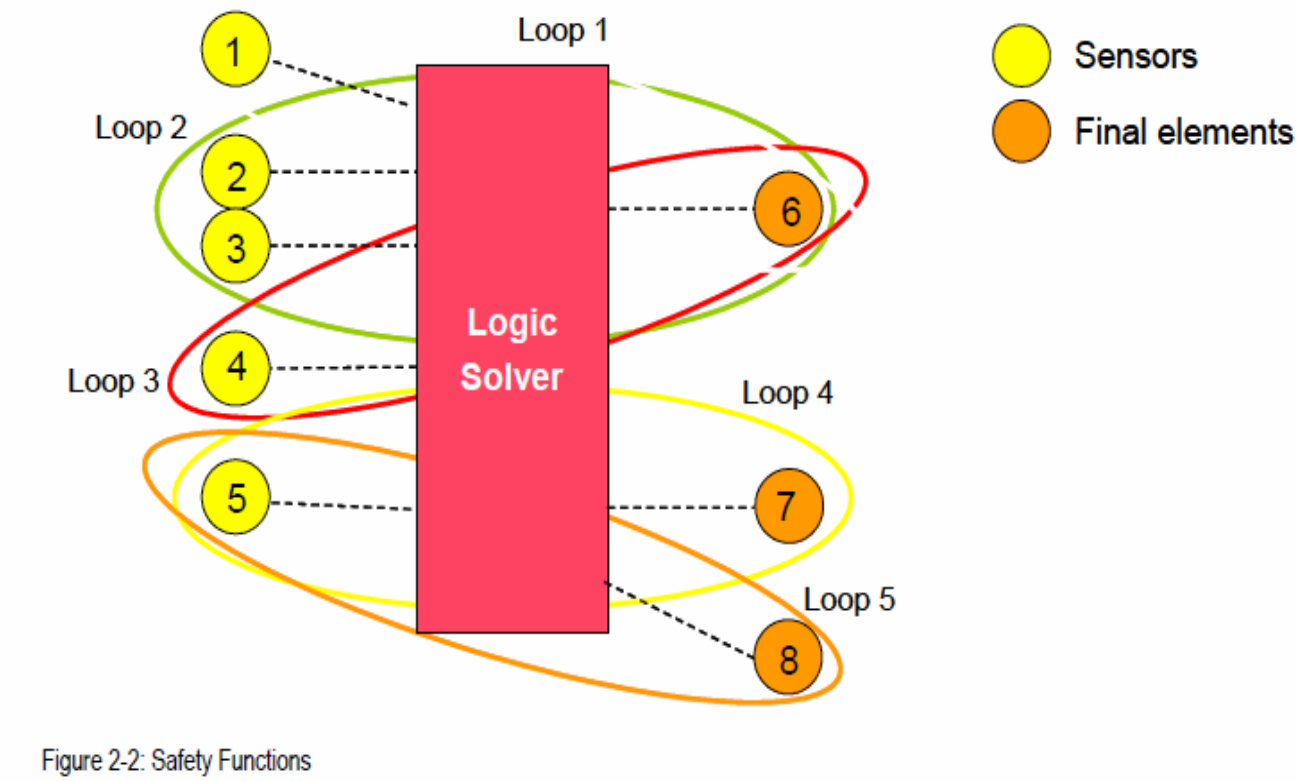
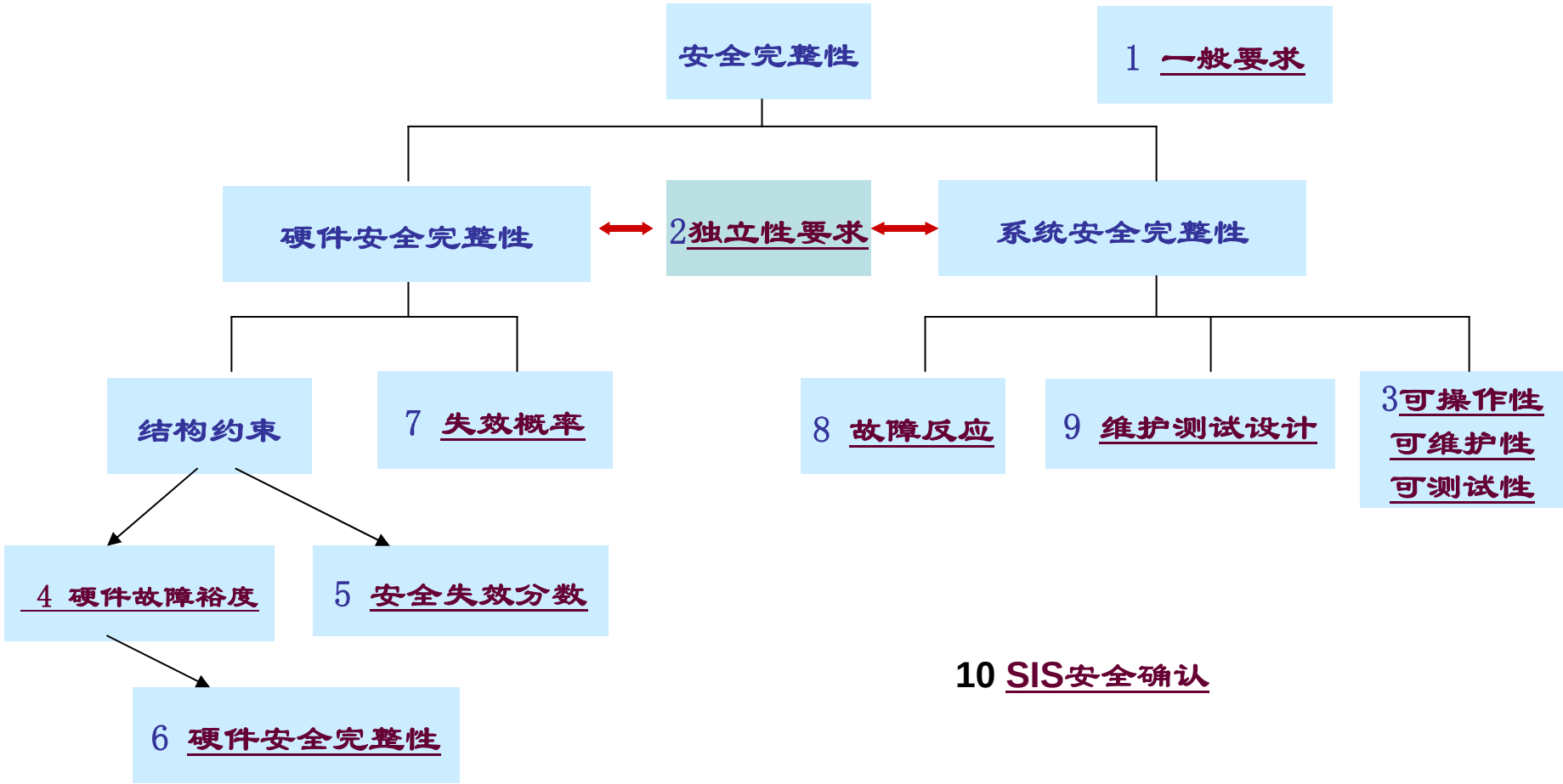


Figure 2-2: Safety Functions

SIL设计与工程



10 SIS安全确认

SIS设计与工程

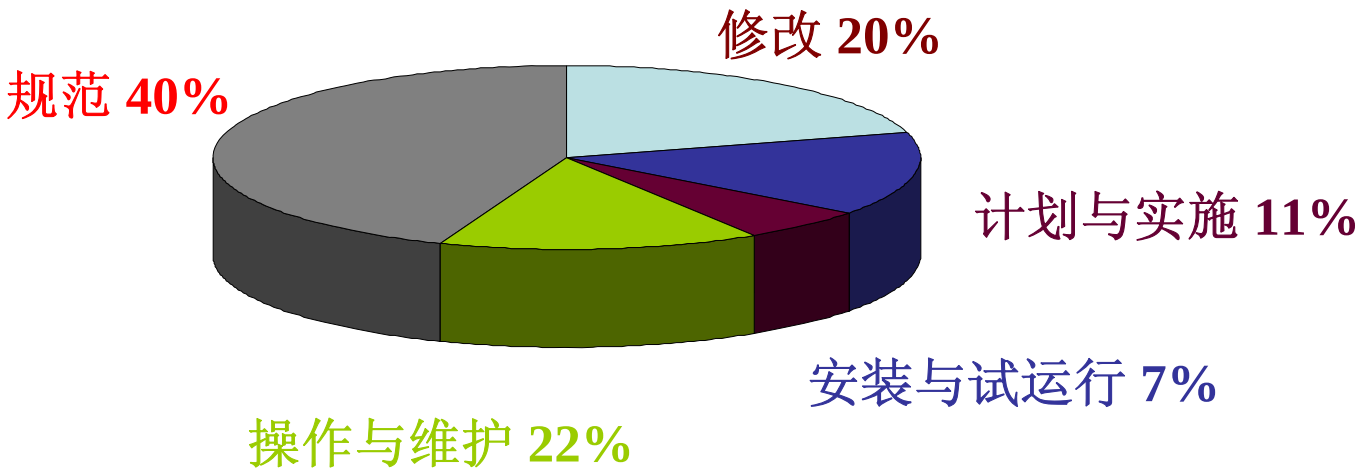
- 1 一般要求
- 2 独立性要求
- 3 可操作性、可维护性、可测试性要求
- 4 硬件故障裕度要求
- 5 安全失效分数要求
- 6 SIF的硬件安全完整性限制
- 7 SIF的失效概率要求
- 8 检测到故障时系统的行为要求
- 9 维护和测试设计要求

1. 一般要求

SIS安全要求规范及设计的基本要求

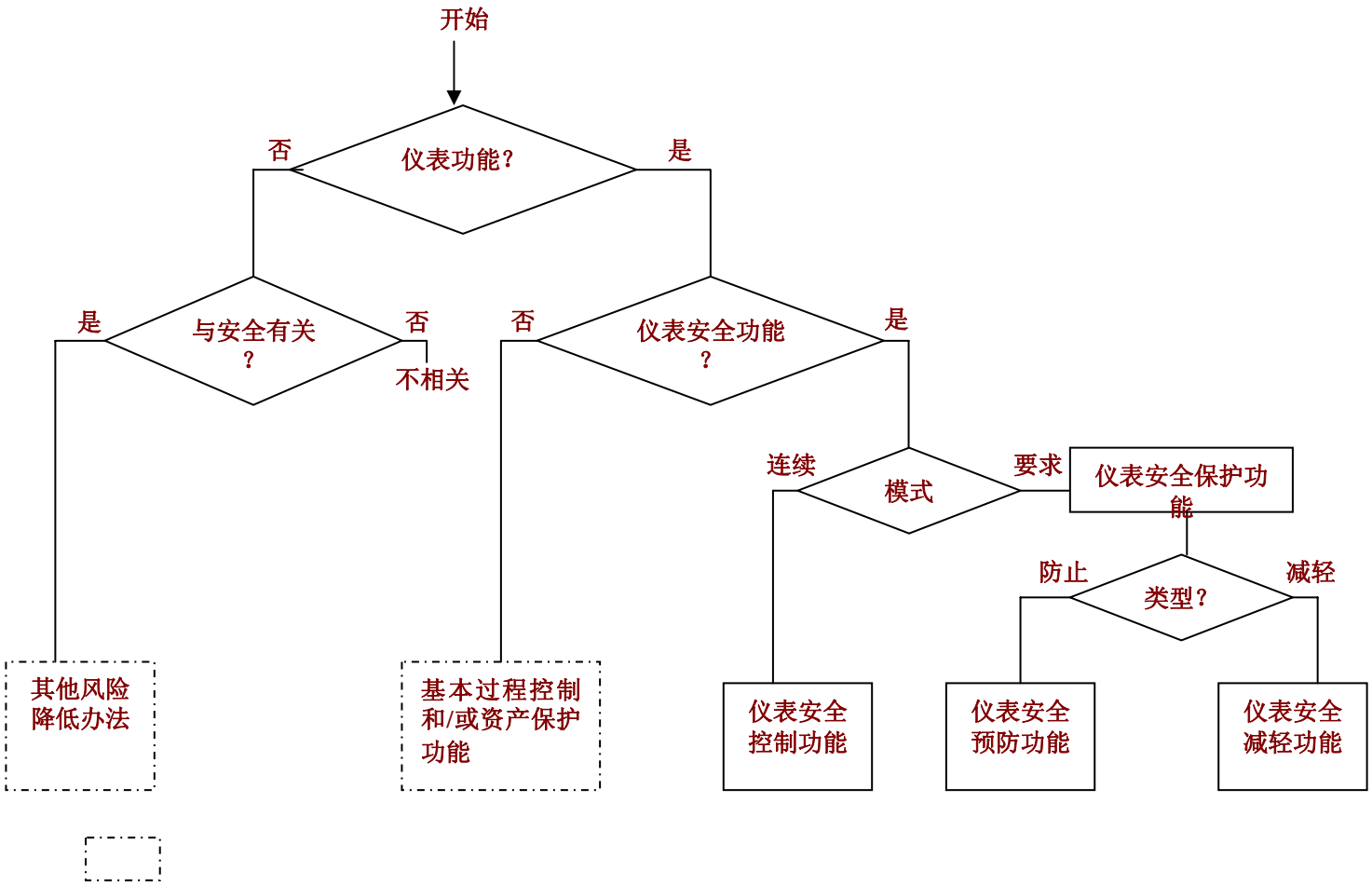
按安全要求规范设计

应根据SIS安全要求规范，并考虑本章的所有要求来设计SIS。



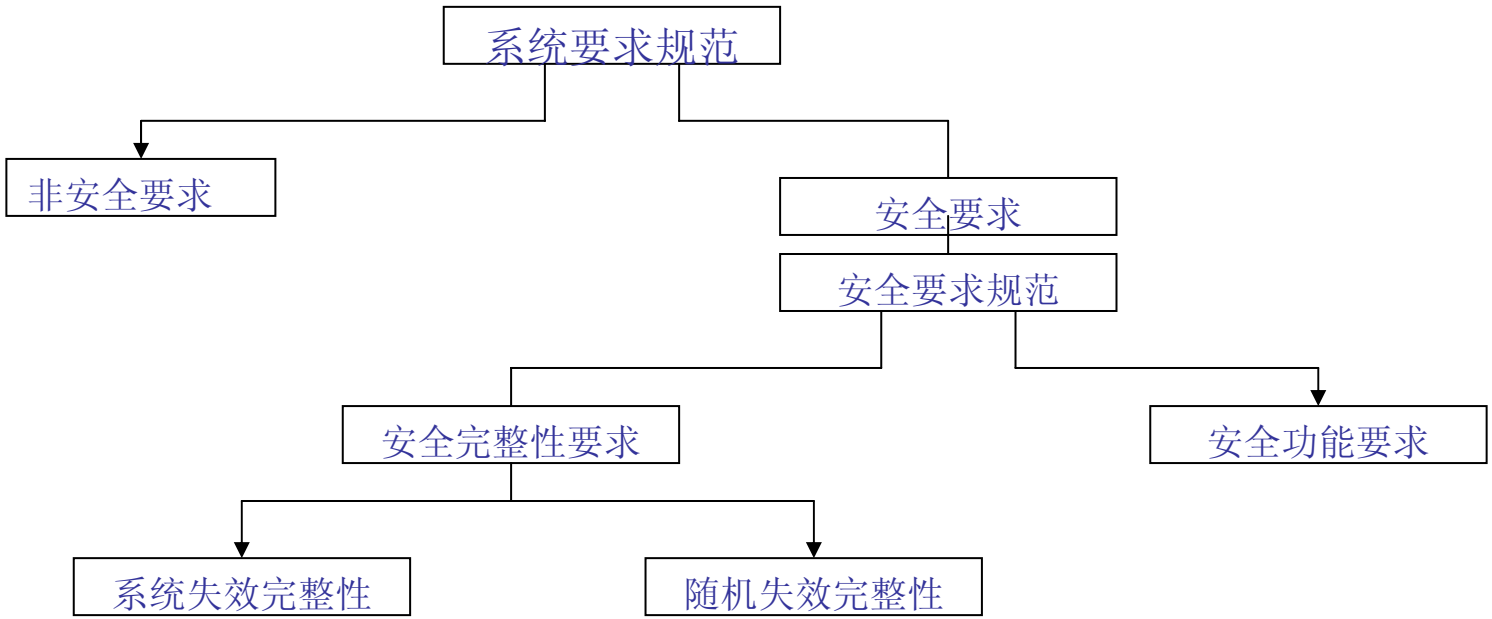
安全要求规范

分清哪些安全功能是由SIS系统完成的



安全要求规范

分清哪些安全功能是由SIS系统完成的



SIS安全要求规范
及设计的基本要求

目　的

目的

- 规定SIF的要求
- 以利于:

  --设计者把这些功能集成到SIS

  --为用户进行SIS的最终工厂验收提供依据

一般要求

一般要求

- 安全要求应从仪表安全功能分配和在安全计划编制过程中确定的那些要求中推导出来。

  注：SIS要求应以下述方法表达和构建：

  — 清楚、精确、可验证、可维护和可行；

  — 易于被在生命周期任何阶段有可能使用这些信息的人理解。

SRS的形式

- 可以是单独一个文档
- 也可以是包含规程、图纸或公司标准惯例的几个文档的一个集合
- 可由危险和风险评估组和/或工程项目组本身拟订这些要求。

SIF要求

SIF安全要求规范

内容:

— 达到要求的功能安全所必需的所有安全仪表功能描述；
— 识别和考虑共同原因失效的要求；
— 对每个所确定的仪表安全功能的过程安全状态的定义；
— 任何单个的过程安全状态的定义，当这些状态同时发生时就会产生一个单独的危险（如应急储存的过载、燃烧系统的多次泄压）；
— 对安全仪表功能提要求和要求率的假定来源；
— 检验测试间隔要求；
— SIS使过程进入某个安全状态的响应时间要求；

SIF安全要求规范

— 每个安全仪表功能的安全完整性等级和操作模式（要求/连续）；
— SIS过程测量和它们的脱扣点（trip point）的描述；
— SIS过程输出动作和成功操作准则的描述，例如紧急关闭截止阀的要求；
— 过程输入和输出之间的功能关系，包括逻辑功能、数学功能和任何要求的许可；
— 人工停机要求；
— 与加电或断电脱扣（trip）有关的要求；
— 在停机后复位SIS的要求；

SIF安全要求规范

— 最大允许虚假脱扣率；
— 失效模式和要求的SIS响应（如报警、自动停机）；
— 与起动和重新起动SIS程序有关的任何特殊要求；
— SIS和任何其他系统（包括BPCS和操作员）之间的所有接口；
— 工厂操作模式的描述，以及每种操作模式下安全仪表功能要求的识别；
—应用软件安全要求；
— 超驰/禁止/旁路要求，包括怎样清除它们；

SIF安全要求规范

— 在检测到SIS中的故障事件时，达到和保持某个安全状态所必需的任何动作的规范。任何这样的动作都应考虑相关人员的因素。
— 在考虑到运输时间、定位、备件安装、服务合同、环境约束时，SIS切实可行的平均修复时间；
— 需要避免的SIS输出状态的危险组合的识别；
— 应识别SIS可能遇到的所有极端环境条件。需考虑的有：温度、湿度、污染、接地、电磁干扰/射频干扰(EMI/RFI)冲击/振动、静电放电、用电区等级、水淹、雷电和其他有关因素；

SIF安全要求规范

— 不论装置作为一个整体（如装置起动）或单个装置操作规程（如设备维护、传感器校准和/或修理），确定其正常和异常模式，需要附加一些安全仪表功能以支持这些操作模式；

— 任何能经受一次重大意外事故的安全仪表功能要求的定义，例如在一次火灾事故中阀门保持可操作性的时间要求。

注：SIS能执行非安全仪表功能以保证有序地停机或较快地起动。这些功能应同安全仪表功能分开。

SIF安全要求规范

- 软件安全要求规范应从安全要求规范和所选定的SIS结构推导出来。

SIS安全要求的应用

SIS安全要求的应用

- 如GB/T 21109.1中描述的那样，有许多需要在项目初期定义的设计要求以确保仪表安全功能提供所要求的保护。
- 各个子系统的安全要求规范也可从这个总体规范中推导出。
- 有关安全要求规范的一些考虑如下：

SIS安全要求的应用

a）需定义的首要条款是仪表安全功能及其安全完整性等级（SIL）。一个仪表安全功能的例子是“通过截断处于高压状态下的进口阀以防止反应釜超压”。典型的功能描述包含：

— 检测危险工况征兆需采取的测量。

一个简单的例子可能是：

检测压力上升超过某个规定值。当压力处于某参数值时应采取动作，该参数值需超过正常操作范围且低于导致危险工况的某个值。需要为系统响应和测量精确度确定一个允许范围。因此，在设置极值时，需要同负责设计和实现安全仪表系统的人员进行讨论；

SIS安全要求的应用

— 防止危险工况需要采取的动作。

一个简单的例子可能是：

在规定的时间内减少流到重沸器（reboiler）的蒸汽流量。

应注意的是，一般仅说明应切断流到重沸器的蒸汽流还是不够充分的。设计师需要知道什么对于成功运行是必要的。例如，根据热负荷，在一分钟之内把流量降低到10%以下就足够了。在其他例子中，可能需要在几秒钟内牢牢地关断蒸汽流；

SIS安全要求的应用

— 不是为了防止危险工况的需要而是可能有利于操作采取的动作。动作可能包括报警、上游或下游单元的关断，以减少对其他保护系统提出要求，或者减少一旦消除了危险的起因则使能快速起动的动作。

值得注意的是，应把这些动作同为防止危险工况的必要动作分开，以便最小化成本和把安全仪表系统的边界限定到必要范围内。边界设定越宽，在要求时的整体失效概率满足与规定的完整性等级相关的要求就显得越困难；

SIS安全要求的应用

— 避免任何已识别出的可导致危险情况的过程状态或者SIS操作顺序；

— 任何由于会导致危险情况而需要被防止的已识别出的过程状态或者SIS操作序列。

b）根据应起动或停止哪个流程、应打开或关闭哪个过程阀门以及任何旋转设备（泵、压缩机和搅拌器）的操作状态，本规范应定义每个已识别出的功能的过程安全状态。如果将一个过程导向安全状态涉及顺序要求，则也应确定该顺序

注：在定义最终元件时，应考虑多样性的好处，例如，关断产品流和关断蒸汽流以降低高压。

SIS安全要求的应用

c）在开始设计SIS时，就应定义所需检验测试间隔的要求，以便在设计中能把它考虑在内。

例如，如果要在计划的停机期间（如每三年）执行检验测试，则设计可能要求比检验测试间隔为一年时更高的冗余程度。

d）应定义能手动使过程进入安全状态的要求。

例如，如果要求操作员能够从控制室或现场手动关闭一台设备，则需对此进行规定。也需规定SIS逻辑解算器的手动停机开关的任何独立性要求。

SIS安全要求的应用

e） 需规定在一次停机之后重新起动过程的所有要求。
例如，某些用户在主控面板上或在现场有电子复位开关，而另有一些用户则可能使用带锁定手柄的螺线管。如果存在类似于这种复位动作的特殊要求，它应是安全要求规范的组成部分。

f） 如果存在一个伪脱扣的目标频率，也应把它作为安全要求规范的一部分进行规定，它将是SIS设计中的一个因素。

SIS安全要求的应用

g）需充分描述SIS和操作员之间的接口，包括报警（预停机报警、停机报警、旁路报警和诊断报警），图形和事件顺序记录。

h） 也可能存在旁路需要以便能在过程运行的同时测试或维护SIS。如果存在旁路诸如键锁或口令这类装置的特殊要求，也需要把这些作为安全要求规范的一部分规定下来。

SIS安全要求的应用

i）应定义SIS的失效模式和对已检测到的故障的响应。

例如，可以把一个变送器设计成失效就面临一次脱扣状态或者失效就解除脱扣状态。如果把它设计成失效就解除脱扣状态，重要的是操作员能得到变送器失效的一个报警以及培训操作员采取必要的纠正动作，以使变送器尽快地得到修复。

关于已检测出的故障的要求，也见GB/T 21109.1的11.3。

2. 独立性要求

独立性要求

- 在要求SIS同时实现安全和非安全仪表功能时，在正常状况下和故障状况下，对任何SIF有负面影响的所有硬件和软件应被当成SIS的组成部分，并符合对最高SIL的要求。

注1：只要可行，就应把安全仪表功能同非安全仪表功能分开。

注2：充分的独立性意味着任何非安全功能的失效或者编程访问非安全软件功能都不能引起安全仪表功能的失效。

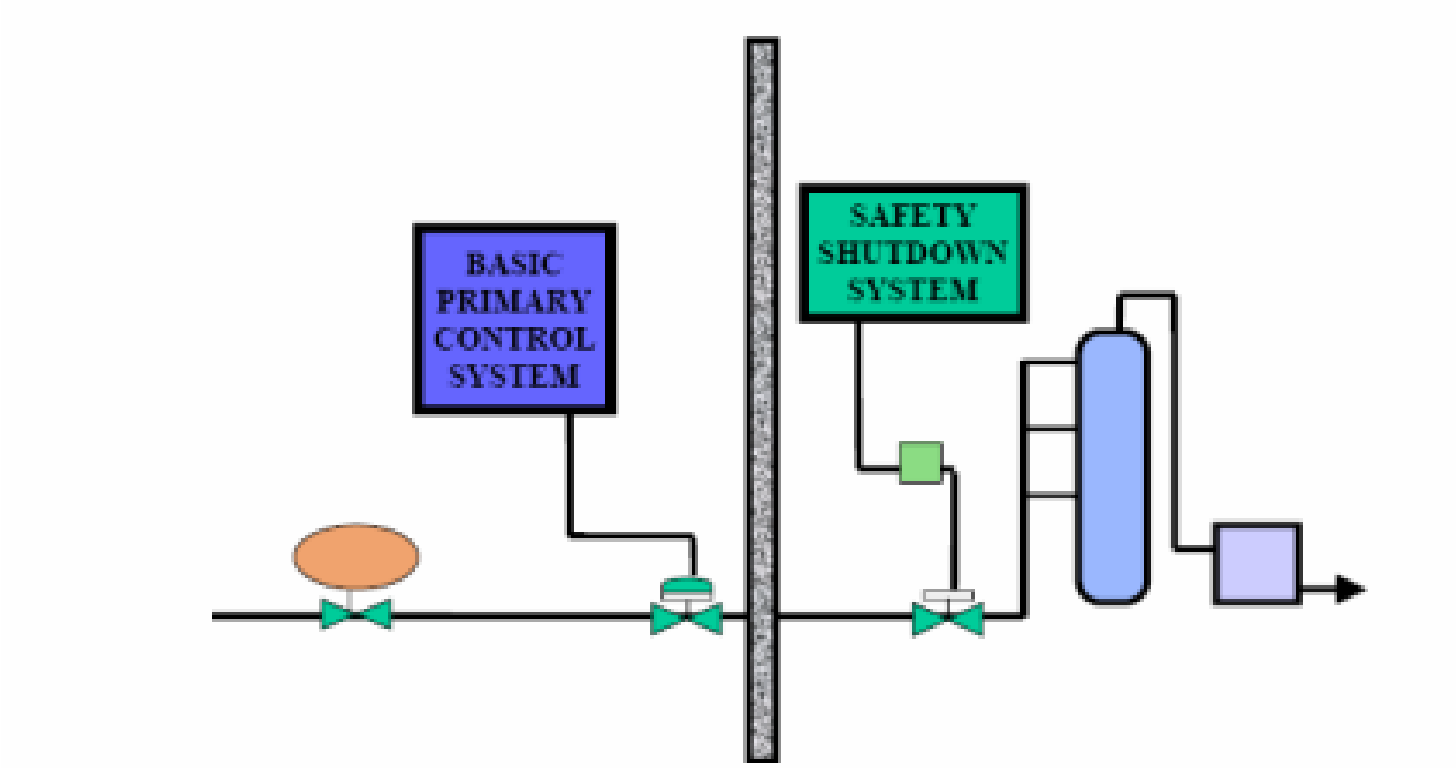
- 在SIS实现不同安全完整性等级的安全仪表功能时，除非能表明较低安全完整性等级的安全仪表功能对较高安全完整性等级的安全仪表功能没有负面影响，否则共享或共用硬件和软件应符合最高安全完整性等级。

- 如果不打算让基本过程控制系统符合本标准要求，基本过程控制系统应设计成分开并独立的，从而不危及安全仪表系统的功能完整性。

注1：可交换操作信息但不能危及SIS的功能安全。

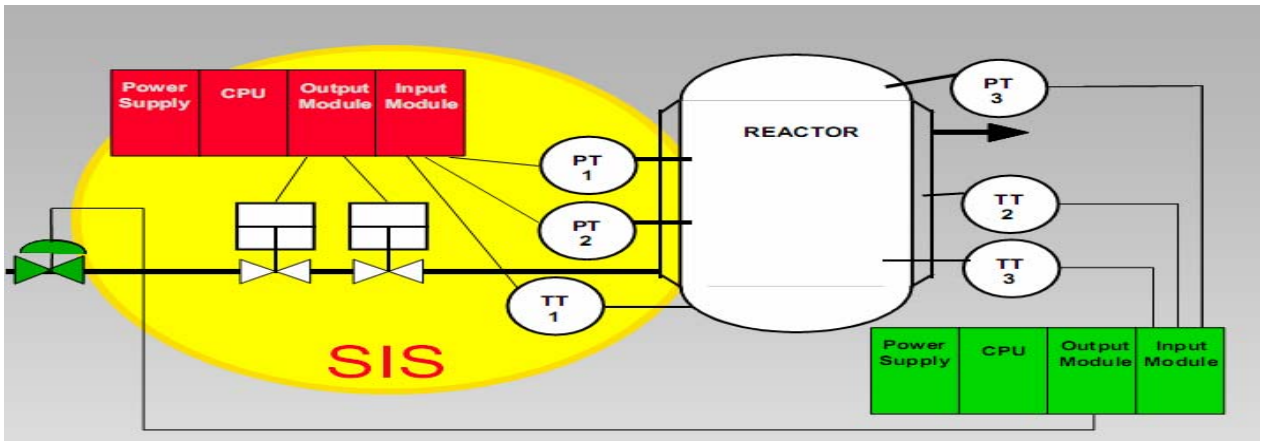
注2：当能表明基本过程控制系统的一次失效不会危害安全仪表系统的安全仪表功能时，SIS的装置也可用于基本过程控制系统的功能。

安全系统与非安全系统的隔离



独立性要求

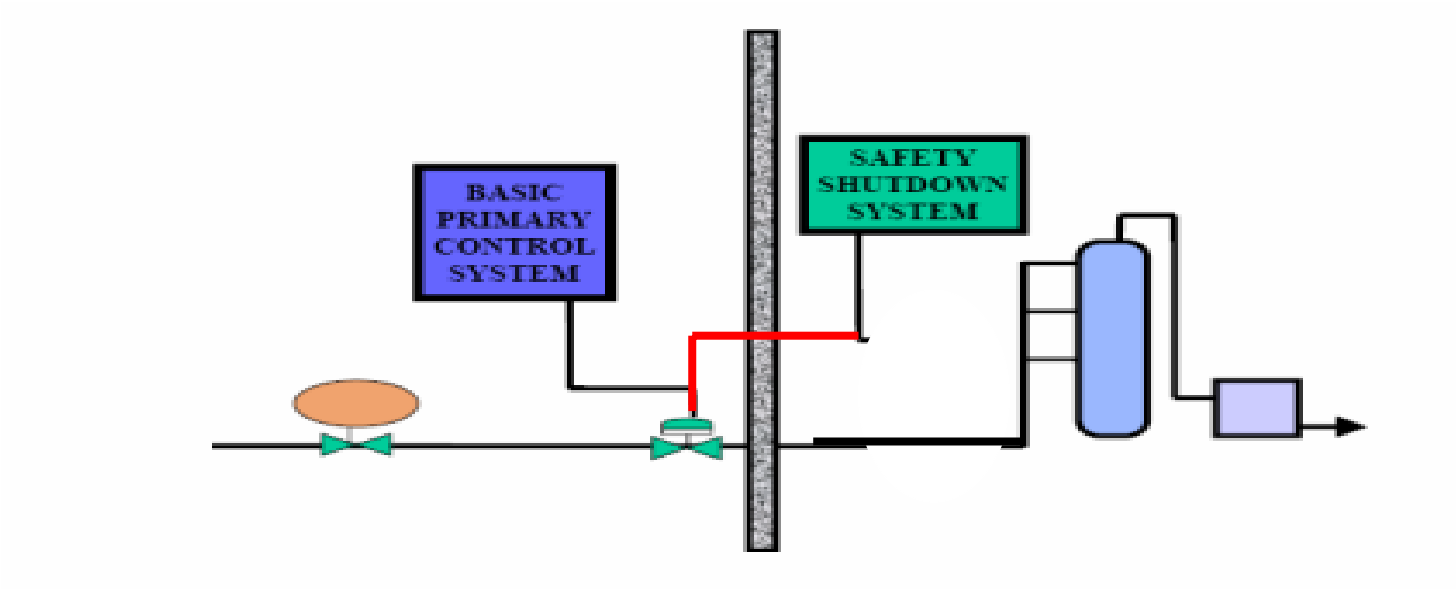
- SIS设计应全面考虑SIS和BPCS之间，以及SIS和其他保护层之间的独立性和相关性的所有方面。
- 一个装置作为执行安全仪表功能的一部分时，不应该（同时）用于基本过程控制目的，因为这个装置失效导致的基本过程控制功能失效，会引起对安全仪表功能的要求。除非分析后可以确认整体风险是可接受的。



BPCS

独立的好处

- 可以降低BPCS对SIS的影响，特别是当它们共享共用装置时。例如，当BPCS和SIS共享一个用于停机和控制的共用阀门时，在该阀门的一次危险失效事件中，它并不能用来执行一个SIS停机功能。



独立的好处

- 可以保持与BPCS有关的更改、维护、测试和文档的灵活性。
- 可以有助于SIS的确认和功能安全评估。

独立的分析

- 在共用装置的一次失效可引起向SIS提出一次要求的情况下，应进行一次分析以保证总危险率满足预期值。总的危险率是共用元件的危险失效率和其他要求源的危险率（包括SIS独立部分的危险失效）的总和。

分离方式的要求

- SIS和BPCS之间的分离可使用同种分离或异种分离。
- 与有助于降低随机失效的同种分离相比，异种分离有利于降低系统失效概率和减小共同原因失效。
- 在SIS和BPCS之间的同种分离在设计和维护时有一些优势，因为它降低了维护错误的可能性，特别是选择在用户组织范围内此前还未使用过的各种部件。
- 虽然要考虑共同原因失效的源头和影响，并且要降低它们的可能性，但对SIL 1、SIL 2和SIL 3而言，SIS和BPCS之间的同种分离是可接受的。

要考虑共因失效

- 共同原因失效的一些例子是：
  - 侵蚀和腐蚀；
  - 由于环境引起的硬件故障；
  - 软件错误；
  - 动力源和供电；
  - 人为错误。
- 异种分离有助于降低系统失效概率（在SIL 3和SIL 4应用中此降低因子特别重要）和减小共同原因失效。

分离的区域

- 一般可供SIS和BPCS进行分离的区域有4个：
- 现场传感器；
- 最终元件；
- 逻辑解算器；
- 配线。

保持独立性的方式

- BPCS和SIS之间也不一定需要物理分离，其条件是它们之间应保持独立性，并且装置安排方式和所使用的规程可以保证SIS不受下列因素的危险影响：
  - BPCS的失效；
  - 在BPCS上进行的作业，如维护、操作或修改。
- SIS设计师需规定可保证SIS不受危险影响应使用的规程

现场传感器应用要求

- BPCS和SIS共用一个传感器时要求进一步地复审和分析。因为此单一传感器的失效可能产生一种危险情况，故有必要进行额外的复审和分析。例如：当BPCS和SIS使用同一个液位传感器，传感器低位失效时，高液位脱扣会产生一次要求。传感器低位失效导致控制器将驱动阀门开启，由于SIS也使用该传感器，而它并不会检测到作为结果而产生的高液位工况。

现场传感器应用要求

- 在一个BPCS和SIS功能使用单一传感器的情况下，一般只有在传感器诊断可把危险失效率降到足够低且SIS能在要求的时间内把过程置于某个安全状态时，才能满足GB/T 21109.1的要求。
- 实际上，即使是在SIL 1应用的情况，也难以达到这一点。对一个SIL 2、SIL 3或SIL 4的仪表安全功能来说，通常需用具有同型或异型冗余的单独SIS传感器来满足要求的安全完整性。

现场传感器应用要求

- 注：当使用一个单独SIS传感器时，通过适当的隔离器把信号转发给BPCS是有好处的。通过对BPCS和SIS传感器之间的信号进行比较，这种安排可能提高诊断覆盖率。
- 当使用冗余SIS传感器时，通过适当的隔离器也可把这些传感器连接到BPCS上。BPCS中的适当算法，通过降低对SIS的要求率，如“取中间值（middle of three）”，可提高安全性。

最终元件应用要求

- BPCS和SIS共用一个阀门的情况大致同共用一个传感器的情况一样，也需要进一步地复审和分析。如果阀门失效将向SIS提出一次要求，通常不推荐SIS和BPCS共用一个阀门。
- 在BPCS和SIS只使用一个阀门的情况下，一般仅当阀门诊断可把危险失效率降到足够低，且SIS能在要求的时间内把过程置于某个安全状态时，才能满足GB/T 21109.1的要求。

最终元件应用要求

- 实际上，即使对SIL 1应用而言，要达到上述要求也是困难的。对一个SIL 2、SIL 3或SIL 4仪表安全功能而言，要满足安全完整性通常需要SIS具有同型或异型冗余的单独阀门。

最终元件应用要求

- 在BPCS和SIS功能使用单一阀门的情况下，设计应保证SIS动作超驰（overrides）BPCS动作。一般可通过把SIS直接连接到一个电磁阀上来达到这个要求，该电磁阀可直接断开执行器的动力源，例如在阀门定位器和执行器之间。

最终元件应用要求

- 当使用冗余SIS阀门时，这些阀门可同时连接到SIS和BPCS上。
- 注：即使使用冗余阀门，考虑BPCS阀门和SIS阀门之间的共同原因失效也是重要的。

最终元件应用要求x

- 确定阀门要求的附加考虑有：
- 截断要求；
- 类似过程应用中阀门可靠性的经验；
- 阀门的非安全失效模式；
- 降低阀门作用的操作规程（例如开启旁路阀门）；
- 检验测试要求。

配线

- 有关给脱扣系统供电的问题，通常BPCS和有关现场设备的配线是同SIS和它的现场设备的配线分开的，这是因为安全功能可能意外失效而不通知脱扣系统。有关这类系统的典型指南包括了安装SIS和BPCS专用的多芯电缆和接线盒。在配线未分开的情况下，为了减少维护中可能产生的错误所导致的SIS失效，建议使用良好的标号和维护规程。
- 给脱扣系统供电涉及到SIF电路，在正常工作状态下，该电路的输出和设备处于断电状态下。施加动力（如电、气体）就产生一次脱扣动作。
- 加电脱扣系统和断电脱扣系统的电缆支持系统（如电缆支架、管道），除另有原因（如电磁干扰）要求分开外，可以共用。关于给脱扣系统供电的问题，可附加对火灾风险区电缆支架防火的考虑。

3. 可操作性、可维护性、可测试性要求

可操作性、可维护性、可测试性要求

- 为了有助于实现设计中的人为因素要求，在设计SIS的过程中，应涉及可操作性、可维修性和可测试性要求（如旁路设施使得在旁路时可进行在线测试和报警）。

注：应设计维护和测试设施，以便把因使用它们而引起的危险失效的可能性减少到切实可行的程度。

用户友善性

- 设计SIS应考虑人的能力和限制。并应适合于分派给操作员和维护人员的任务。所有的人—机接口设计应遵循良好的人员操作惯例，并应适合操作员可接受的培训或认知水平。
  - 应注意人可能犯错，如：
    - 设计中未检测到的错误；
    - 操作中的错误（如错误的设定值）；
    - 维护不当（例如用一个失效动作不正确的阀门来替换另一个阀门）；
    - 校准、测试或解释控制系统输出时的错误；
    - 不能正确响应一次紧急事件。

复位/重启的安全要求

- SIS应设计成只要SIS把过程置于某个安全状态，就会保持在安全状态直到启动一次复位为止，安全要求规范另有规定的情况除外。
  - 一般应只有在操作员的手动动作之后，才可能重新起动。

手动机制

- 与逻辑解算器无关的手动机制（如应急停机按钮）应用来启动SIS的最终元件，安全要求规范另有规定的情况除外。
  - 手动意味着SIS逻辑解算器和BPCS控制系统二者是独立的，配备它们是为了在发生一次紧急事件时操作员能够启动停机。在SRS中通常定义有手动停机的要求。
  - 倘若必要并且危险和风险评估组认为合适，就可把紧急停机连接到SIS PE逻辑解算器（例如当要求按顺序停机时）。

手动机制

- 独立性经验法则
  - 如果SIL1或者SIL2的功能在SIL3的逻辑控制器中实施,手动关闭可以通过逻辑控制器实施
  - 如果SIL3在SIL3逻辑控制器内,手动关闭必须独立于逻辑解算器
- 在安全要求规范中要定义手动关闭.

对掉电-安全子系统的要求

对掉电时不丧失安全状态的子系统而言，应满足下列所有要求

- 电路完整性丧失的检测（如线路终端监视）；
- 使用辅助电源（如备用电池，不间断电源）保证电源完整性；
- 子系统掉电的检测。
- 并按“检测到故障时系统行为的要求”采取动作

在失去动力源的最终元件失效后不能进入安全状态（例如给脱扣系统供电）的情况下，应考虑包含本地手动方式达到安全状态的条款。

4. 硬件故障裕度要求

硬件故障裕度要求

对安全仪表功能而言，其传感器、逻辑解算器和最终元件应具有最低的硬件故障裕度。

硬件安全完整性的结构约束

硬件安全完整性的安全功能所声明的最高安全完整性等级，受限于硬件故障裕度和执行该安全功能的子系统的安全失效分数。

对于这些要求：

a. 硬件故障裕度N意味着N+1个故障会导致全功能的丧失，在确定硬件故障裕度时不考虑其它可能控制故障影响的措施，如诊断；

b. 若一个故障可直接引起一个或几个后续故障的发生，这些故障可视为单个故障；

c. 在确定硬件故障裕度时，如果相对于子系统安全完整性而言某些故障出现的可能性很小，这些故障可不考虑。不考虑这类故障的合理性应被证明和文档化。

d. 子系统安全失效分数的定义为子系统的平均安全失效率加检测到的平均危险失效率与子系统总平均失效率之比。

A类子系统的概念

满足下列条件，其部件被要求达到安全功能的一个子系统可视为A类

a) 所有组成部件的失效模式都被很好地定义；并且

b) 故障状况下子系统的行为能够完全确定；并且

c) 通过现场经验获得充足而可靠的数据，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。

典型A类设备：开关、气动增压器、执行器、阀门、继电器，或由电阻、电容放大器等构成的简单电子模块

B类子系统概念

满足下列条件，其部件被要求达到安全功能的一个子系统可视为B类：

a)至少一个组成部件的失效模式未被很好地定义；或

b)故障状况下子系统的行为不能完全确定；或

c)通过现场经验获得的可靠的数据不够充分，不足以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。

典型B类子系统：基于微处理器的设备，或具有复杂自定义逻辑的设备

硬件安全完整性:A类安全相关子系统的结构约束

安全失效分数	硬件故障裕度（见注2）		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% - <90%	SIL2	SIL3	SIL4
90% - <99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4
注1：本表的详细解释见7.4.3.1.1~7.4.3.1.4。 注2：硬件故障裕度N表示N+1个故障将导致安全功能的丧失。 注3：如何计算安全失效分数见附录C。			

硬件安全完整性：B类安全相关子系统的结构约束

安全失效分数	硬件故障裕度		
	0	1	2
<60%	不允许	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

注：B类的含义:a.至少一个组成部件的失效模式未被很好地定义；
b.故障状况下子系统的行为不能完全确定；或
c.通过现场经验获得的可靠的数据不够充分，不足以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

PE逻辑解算器的最低硬件故障裕度

SIL	最低硬件故障裕度		
	SFF<60%	SFF 60%～90%	SFF>90%
1	1	0	0
2	2	1	0
3	3	2	1
4	应用特殊要求（见 GB/T 20438－2006）		

SFF:安全失效分数

传感器、最终元件和非PE逻辑解算器的最低硬件故障裕度

SIL	最低硬件故障裕度（见 11.4.3 和 11.4.4）
1	0
2	1
3	2
4	应用特殊要求（见 GB/T 20438－2006）

传感器、最终元件和非PE逻辑解算器的最低硬件故障裕度

假设SFF<60%,简单子系统

■结构约束 - 复杂子系统

Safe failure fraction 安全失效分数SFF	Hardware fault tolerance 硬件故障裕度HFT		
	0	1	2
< 60 %	不允许	SIL 1	SIL 2
60 % - ≤ 90 %	SIL 1	SIL 2	SIL 3
90 % - ≤ 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

例：某设备安全失效分数为92%，HFT=0，则SIL为2

例2：某B类设备的SFF为50%，安全仪表功能的目标SIL为1，则该设备子系统需要1oo2/2oo3的冗余配置。

HFT与冗余

Hardware Fault Tolerance(硬件故障裕度 HFT)

HFT = 0 单通道系统

HFT = 1 冗余系统

HFT= 2 三重冗余

1oo3 → **HFT=2**

2oo3 → **HFT=1**

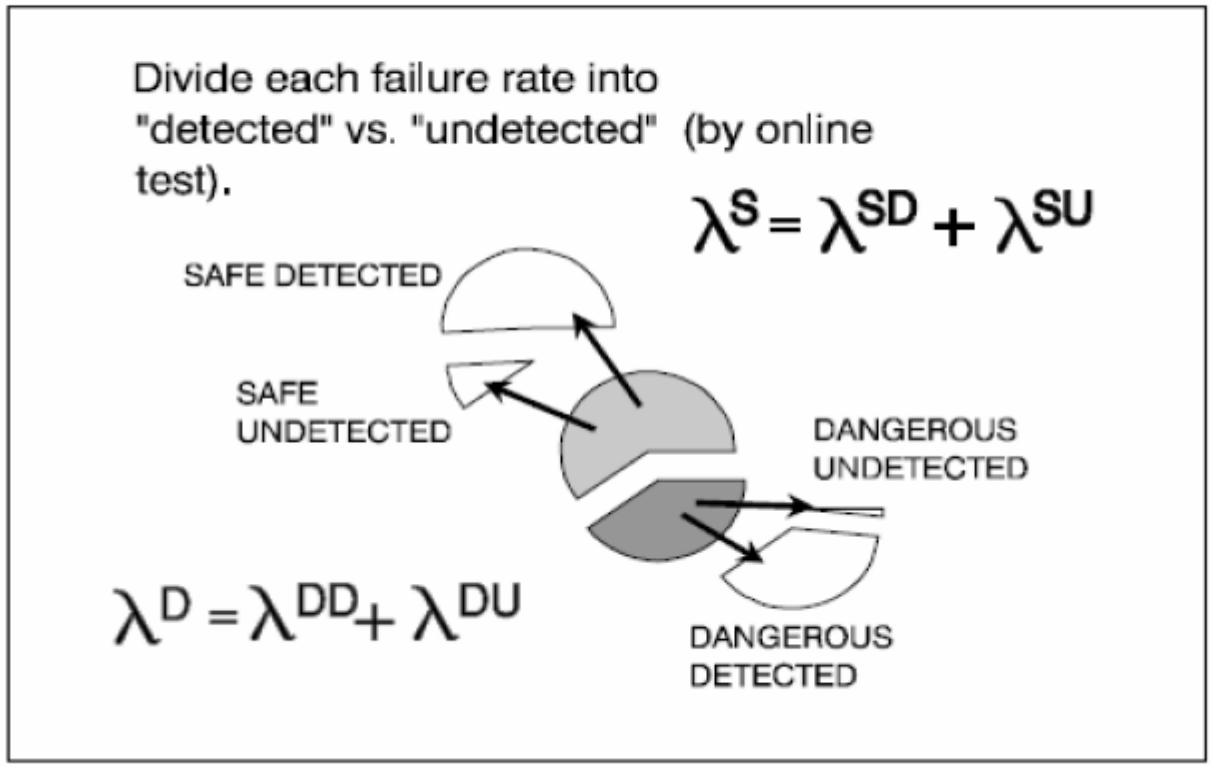
三个通道

3oo3 → **HFT=0**

5. 安全失效分数要求

安全失效分数

PFD = f (failure rate, repair rate, test interval, common cause, etc.)



■Safe Failure Fraction(安全失效分数SFF)

一个子系统的SFF被定义为:

$$(\sum \lambda_S + \sum \lambda_{DD}) \ / \ (\sum \lambda_S + \sum \lambda_D)$$

λ_S ： 安全失效率

λ_D ： 危险失效率

λ_{DD} ： 内部诊断检测到的危险失效率

诊断覆盖率(Diagnostic coverage factor) DC

- 危险失效又被分为检测到的危险失效λ_{DD}与未检测到的危险失效 λ_{DU}
- 取决于故障检测措施的有效性,对系统中每一个单独部件都要评估DC

$$\lambda_{DD} = \lambda_D \cdot DC$$
$$\lambda_{DU} = \lambda_D \cdot (1 - DC)$$

Example：FlashROM

检验和：Max claimed DC=60%

8bit-CRC:99.6%　　16bit-CRC：99.998%

SFF计算示例

$$SFF = \frac{\Sigma \lambda_S + \Sigma \lambda_{DD}}{\Sigma \lambda_S + \Sigma \lambda_{DD} + \Sigma \lambda_{DU}}$$

例：

单元：FIT（10E-09）

器件	λ	DC	λS	λDD	λDU	λS＋λDD
①	200	60％	100	60	40	160
		99％	100	99	1	199
②	100	90％	50	45	5	95

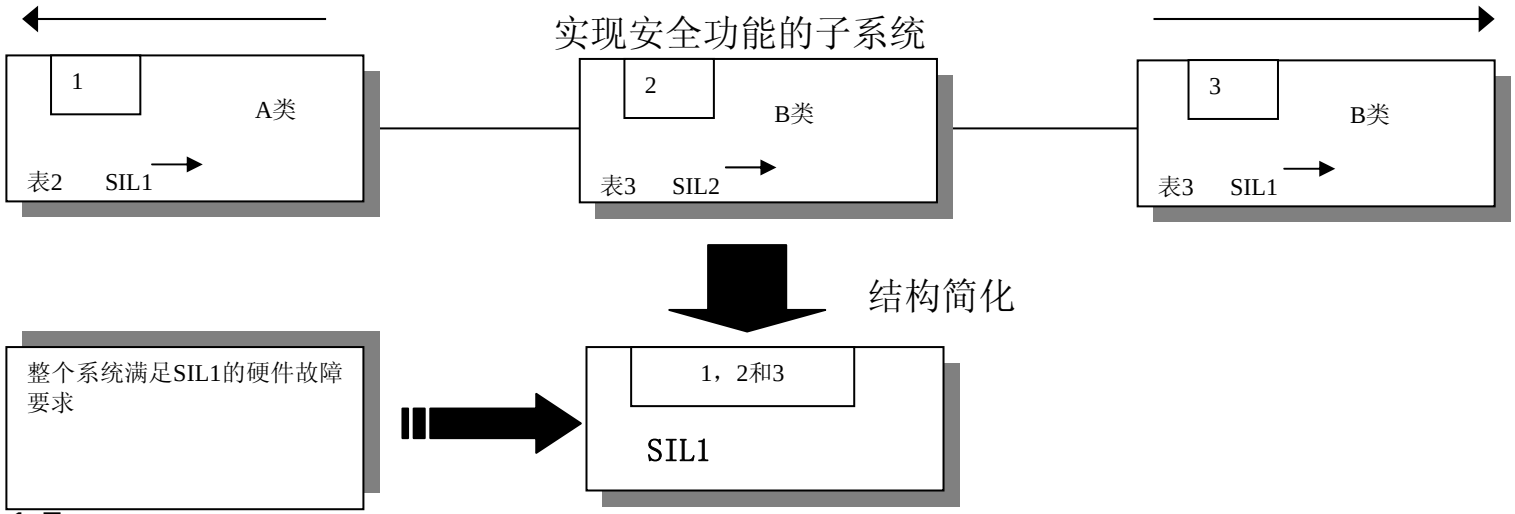
例1：SFF＝((100+50)＋(60+45))/(200+100)=85%

例2：SFF＝((100+50)＋(99+45))/(200+100)=98%

6. SIF的硬件安全完整性限制

单通道安全功能的硬件安全完整性限制

在SIS中，若某安全功能是通过单一通道实现的，该安全功能所能声明的最大硬件安全完整性等级取决于能满足最低硬件安全完整性等级要求的子系统。



多通道安全功能的硬件安全完整性限制

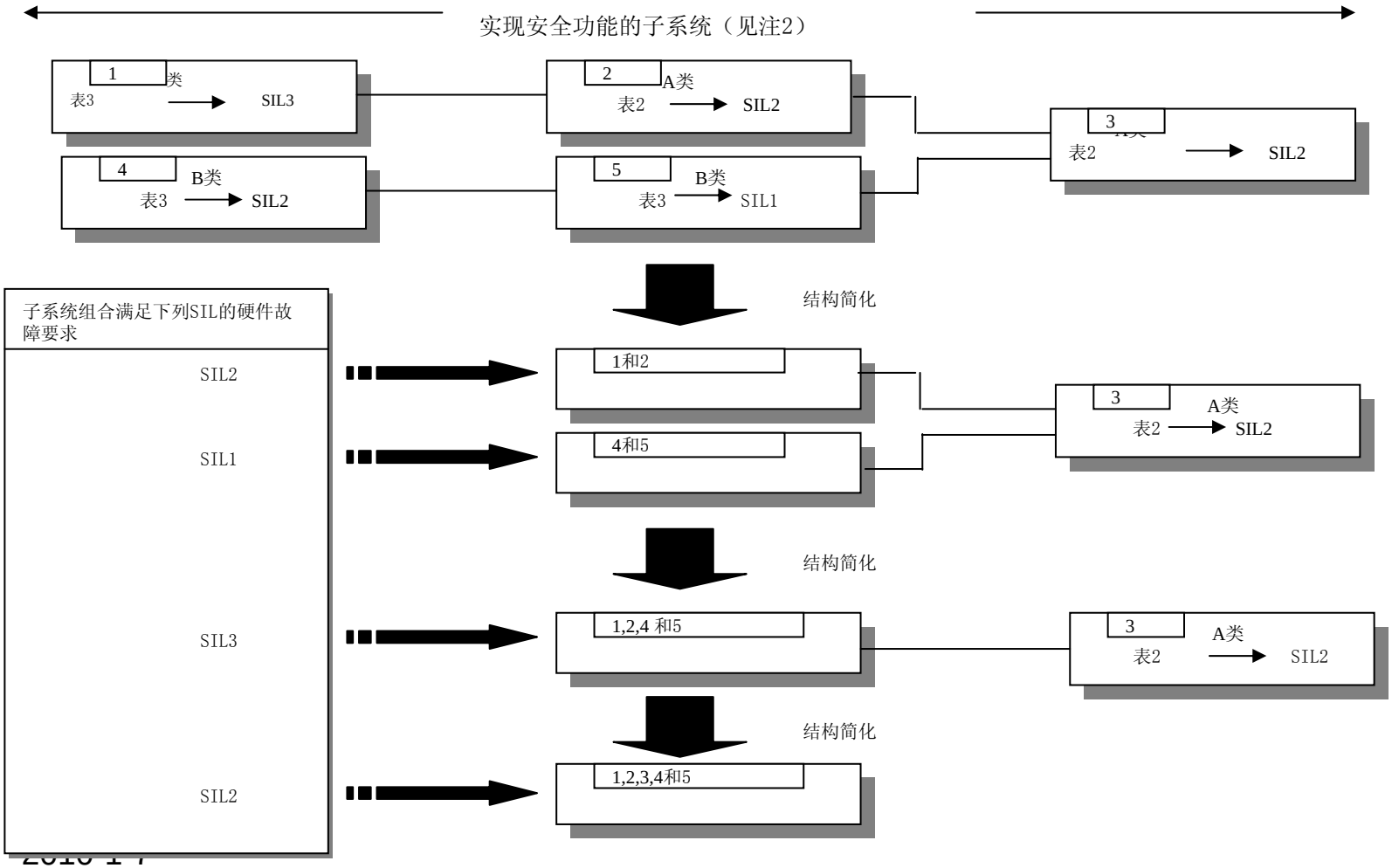
在SIS中，若某个安全功能是通过其子系统的多个通道实现的，该安全功能所能声明的最大硬件安全完整性等级取决于：

a) 根据表2或表3的要求评估每一子系统，并且

b) 将子系统组成为组合；并且

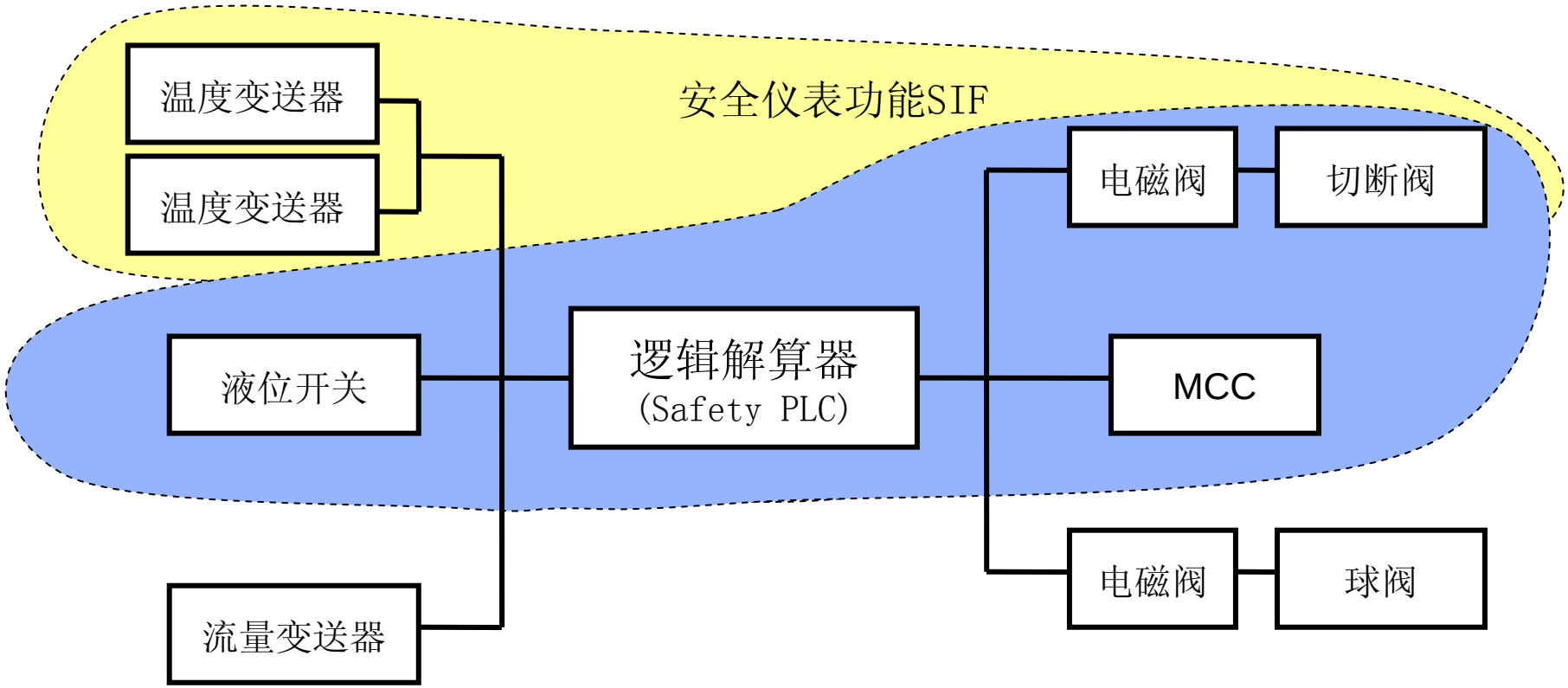
c）分析这些组合以确定整体硬件安全完整性等级。

多通道安全功能的硬件安全完整性的限制示例



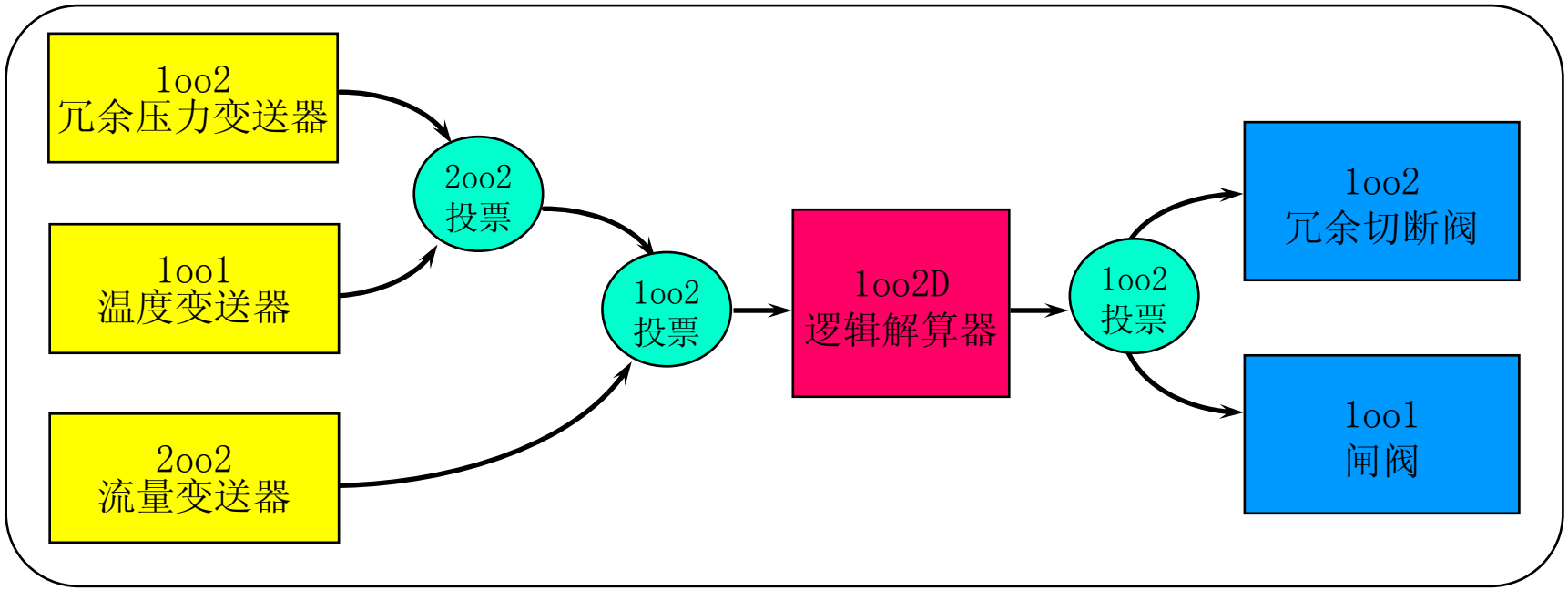
7. SIF的失效概率要求

安全仪表功能



安全仪表系统SIS

复杂的安全仪表功能


1oo2
冗余压力变送器
1oo1
温度变送器
2oo2
流量变送器
2oo2
投票
1oo2
投票
1oo2D
逻辑解算器
1oo2
投票
1oo2
冗余切断阀
1oo1
闸阀

安全功能的目标失效量

1) 以低要求操作模式工作的**E/E/PE**安全相关系统

PFD

安全完整性水平 (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

2)以高要求或连续模式工作的 **E/E/PE**安全相关系统

PFH

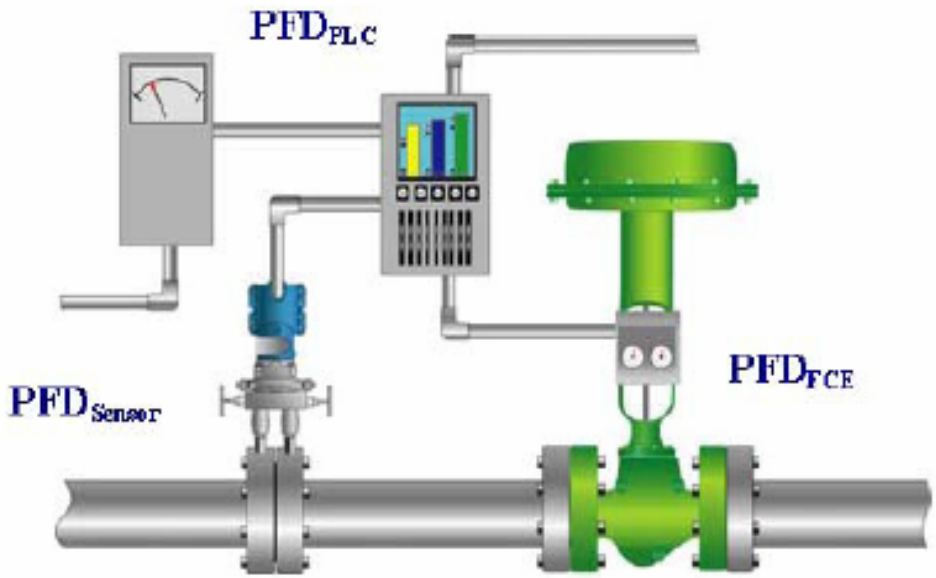
Safety integrity level (SIL)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

安全功能的目标风险降低

安全仪表功能（SIF）提供的风险降低要求与SIL的对应关系

安全完整性水平 (SIL)	目标风险降低
4	≥ 10 000 to < 100 000
3	≥1 000 to < 10 000
2	≥100 to <1 000
1	≥ 10 to <100

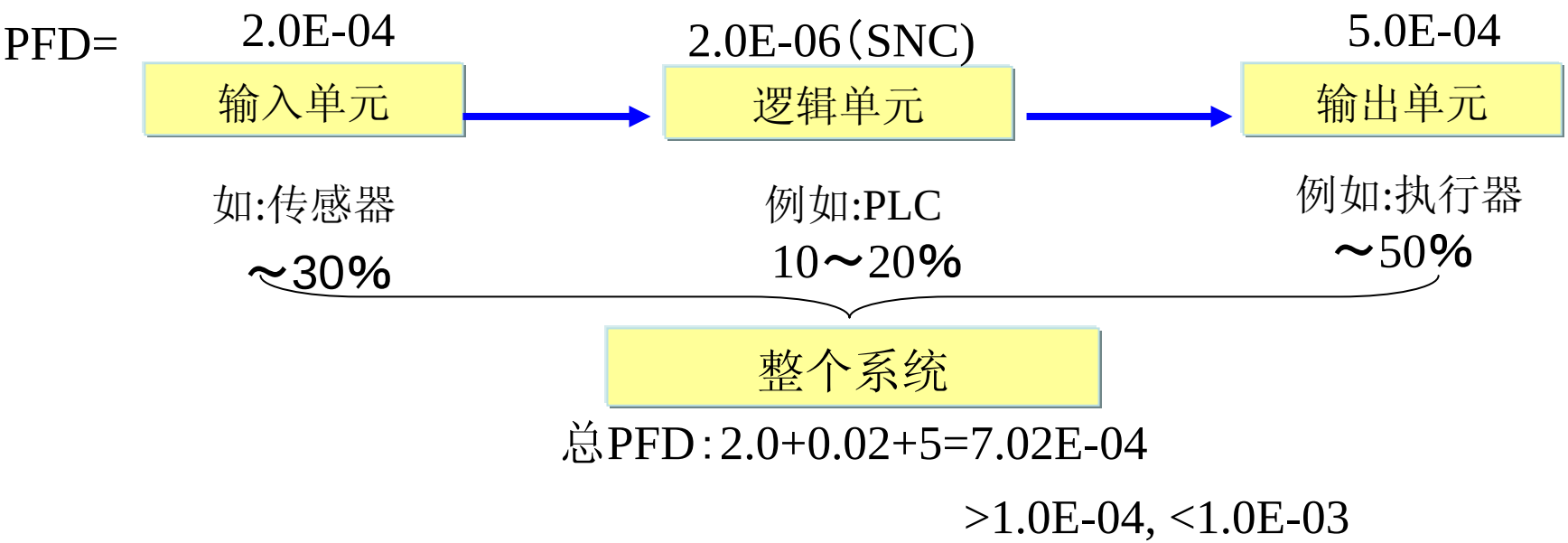
整个回路 PFD计算



Total Loop SIL =
PFD_{PLC} + PFD_{Sensor} +PFD_{FCE}

安全回路PFD计算实例

检验测试间隔时间 = 1年 ＝8760小时



SIL3

目标失效量

每个安全仪表功能在要求时的失效概率应等于或小于安全要求规范中所规定的目标失效量。通过计算可对此进行验证。

注1：在要求操作模式下运行的安全仪表功能，应使用在要求时执行其设计功能的平均失效概率来表示目标失效量，如安全仪表功能的安全完整性等级所确定的那样（见表3）。

注2：在连续操作模式下运行的安全仪表功能，应使用每小时的危险失效频率来表示目标失效量，如安全仪表功能的安全完整性等级所确定的那样（见表4）。

注3：因为使用了不同的部件失效模式并且SIS的结构（用冗余表示）也可能有变化，所以对每个安全仪表功能的失效概率单独定量是必要的。

注4：目标失效量可以是要求时的平均失效概率的某个规定值，或者是根据定量分析得出的危险失效率的某个规定值，或者是由定性方法确定的与SIL相关的一个规定范围。

失效概率计算需要考虑的要素

由硬件失效算出的每个安全仪表功能的失效概率应考虑：

a）SIS的结构，这是由于它同所考虑的每个安全仪表功能有关；

b）估计的每个子系统的失效率，它是由任何模式下的随机硬件故障产生的，这种故障可引起SIS的一次危险失效且已被诊断测试检测到；（ λ_{DD} ）

c）估计的每个子系统的失效率，它是由任何模式下的随机硬件故障产生的，这种故障可引起SIS的一次危险失效且未被诊断测试检测到；（ λ_{DU} ）

失效概率计算需要考虑的要素

d）SIS对共同原因失效的敏感度；

e）任何定期的诊断测试的诊断覆盖率（按GB/T 21109.2确定的），相关的诊断测试间隔和诊断设施的可靠性；

f）进行检验测试的时间间隔；

g）已检测到的失效的修复时间；

失效概率计算需要考虑的要素

h)在任何模式下可能引起SIS一次危险失效的任何通信过程的估计危险失效率（包括诊断测试检测到的和未检测到的两种情况）；

i）在任何模式下可能引起SIS一次危险失效的任何人为响应的估计危险失效率（包括诊断测试检测到的和未检测到的两种情况）；

j）对电磁兼容性（EMC）干扰的敏感度（例如符合GB/T 18268）；

k）对气候和机械条件的敏感度（例如符合GB/T 17214.1－1998和IEC 60654-3:1998）。

失效概率计算需要考虑的要素

注1：应提供建模方法，选择最合适的方法是分析人员的责任并同具体情况有关。适用的方法包括（见GB/T 20438.6－2006附录B）：

- 仿真；
- 因果分析；
- 故障树分析；
- 马尔可夫（Markov）模型；
- 可靠性方框图。

注2：诊断测试间隔时间加上修理持续时间构成了平均恢复时间（见IEV 191-13-08），在可靠性模型中应考虑它。

8. 检测到故障时系统的行为要求

检测到故障时系统行为的要求

在能允许单一硬件故障的任何子系统中，检测到危险故障时（利用诊断测试、检验测试或任何其他办法）应导致：

a）执行一个规定动作，以达到或保持安全状态；或者

b）在修复故障部分的同时继续过程的安全运行。如果故障部分的修复不能在计算硬件随机失效概率中假定的平均恢复时间（MTTR）内完成，则会产生一个规定的动作以达到或保持某个安全状态。

注：在安全要求规范中，应规定为达到或保持某个安全状态所需的规定动作（故障反应）。例如，它可以是过程或过程的某个部分的安全停机。

在上述动作有赖于操作员为响应一次报警而采取的特定动作（如打开或关闭一个阀门）的情况下，则应把报警当成安全仪表系统的一部分（即BPCS的独立性）。

在上述动作有赖于操作员为响应诊断报警而通知维护以便修复一个故障系统的情况下，该诊断报警可以是BPCS的一部分，但应经受适当的检验测试，并随SIS的其余部分一起进行变更管理。

检测到故障时系统行为的要求

如果该子系统是无冗余的、安全仪表功能完全依赖于该子系统，且子系统仅按要求模式实现安全仪表功能的情况下，当在子系统中检测到危险故障时（利用诊断测试、检验测试或任何其他办法），则应导致：

a）执行一个规定动作，以达到或保持安全状态；或者

b）在计算硬件随机失效概率中假定的平均恢复时间（MTTR）时段内修复故障子系统。在这段时期应由附加的措施和约束保证过程持续安全。这些措施和约束提供的风险降低，至少应等于无任何故障时的安全仪表系统所提供的风险降低。在SIS操作和维护程序中应规定这些附加措施和约束。如果不能保证在规定的平均恢复时间（MTTR）内完成修复，则应执行一个规定动作以达到或保持某个安全状态。

检测到故障时系统行为的要求

如果该子系统是无冗余的、安全仪表功能完全依赖于该子系统，且子系统仅按连续操作模式实现所有安全仪表功能的情况下，当在子系统中检测到危险故障时（利用诊断测试、检验测试或任何其他办法），则应导致一个规定动作，以达到或保持某种安全状态。

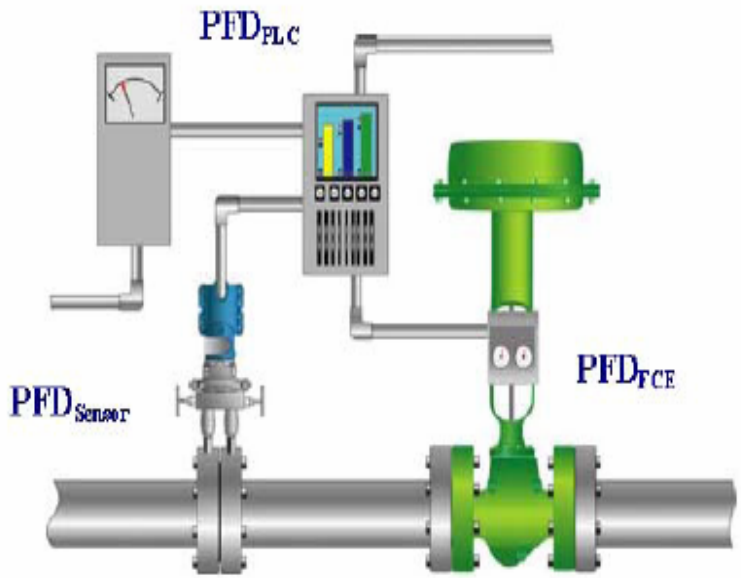
注：当一个子系统的输出状态的一些组合有可能直接引起一个危险事件时，需要把子系统中的危险故障检测看作在连续模式下操作的一个安全仪表功能。

9. 维护或测试设计要求

一般要求

设计应允许对SIS进行端到端的测试或分几部分测试。在预定的过程停机间隔大于检验测试间隔的情况下，需要在线测试设施。

注：术语端到端意味着从传感器端的过程流到执行器端的过程流。



一般要求

- 设计SIS应考虑怎样维护和测试系统。如果要在过程运行的同时测试SIS，设计不应要求断开线路、使用跳线或者强制软件寄存器，因为使用这些技术可能要危及SIS的完整性。为了安全地完成包括传感器、逻辑解算器和最终元件在内的整个系统的测试，系统设计应提供SIS的技术要求和规程要求。

一般要求

- 定义怎样在过程运行的同时维护一个SIS是重要的。例如，如果一个变送器或阀门需要持续运转，则需提供有关在保持过程安全的同时维护部门应怎样处理这些仪表而又不会引起一次乱真脱扣的考虑。

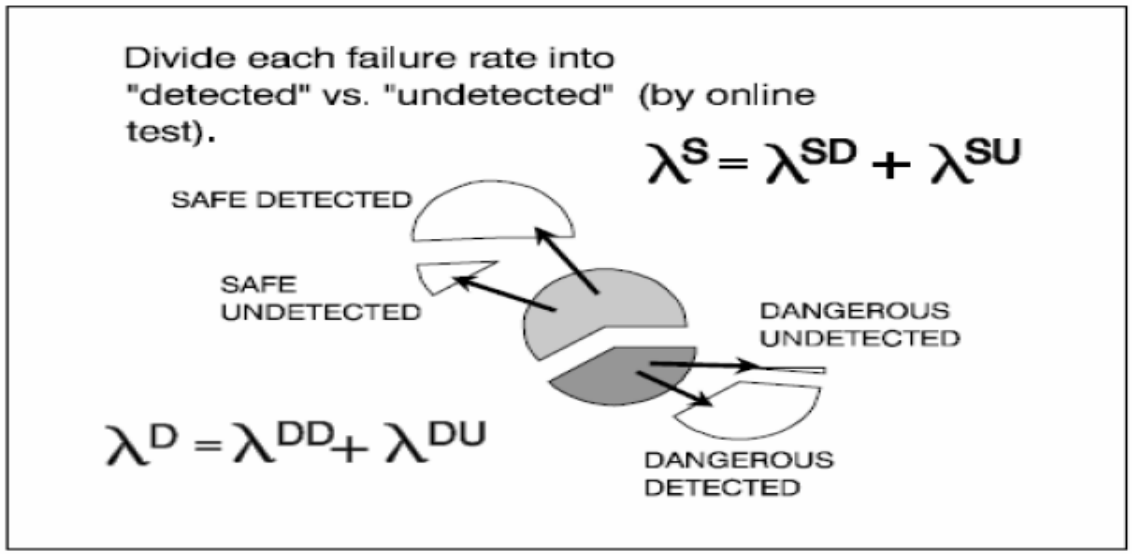
一般要求

- 对最终元件测试周期的任何限制都应在计算SIF的PFDavg时加以考虑。

对在线检测的要求

当要求在线检验测试时，测试设施应是SIS的一部分。测试设施被设计用来测试未揭露的失效。

PFD = f (failure rate, repair rate, test interval, common cause, etc.)



对测试和/或旁路设施要求

当测试和/或旁路设施被包括在SIS中时，它们应符合：

——应按安全要求规范所定义的维护和测试要求设计SIS；

——SIS任何部分的旁路，应通过报警和/或操作规程警告操作员。

对带测试和/或旁路设施的要求

- 安装旁路可能降低一个SIS的保密水平。通过以下办法可以克服保密性的这种降低：
  - 使用口令和/或键锁开关。有些设计可结合带锁机柜内装适当的旁路。
  - 通过对阀门位置加封或者设置指示相应位置的重要性的安全符号，清楚地标识管道旁路。

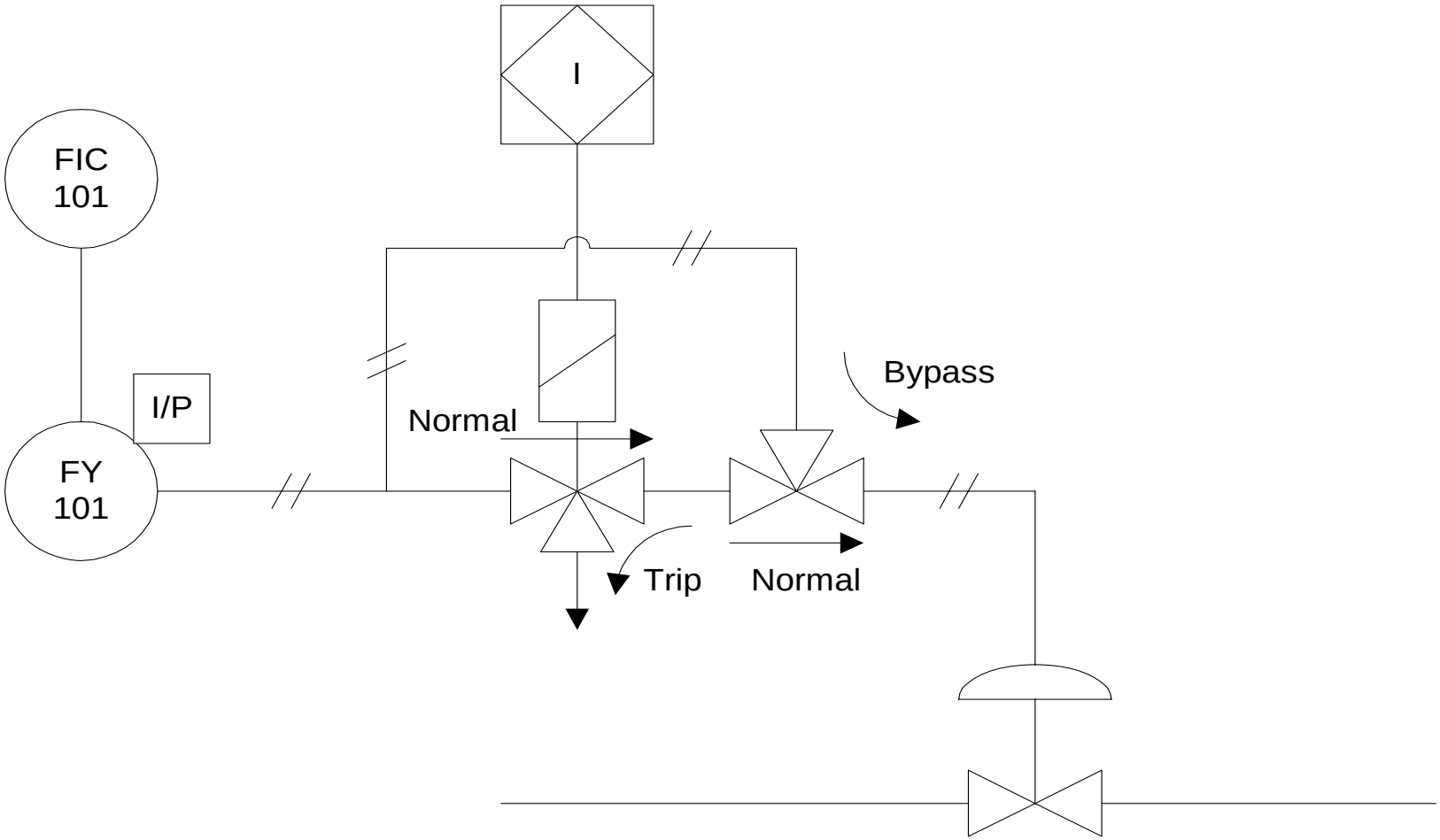
对带测试和/或旁路设施的要求

- 例如，对一个1oo2传感器配置而言，有些用户可能同时旁路两个传感器，而另一些用户可能对每个传感器单独旁路。如果同时旁路传感器，则必须使措施到位以保证风险保持在可允许的范围。两种情况都有可能，应在设计初期就对此进行讨论。

对带测试和/或旁路设施的要求

- 有一些过程操作不支持在过程运行期间移动阀门，或可能在阀门周围安装旁路不现实。在这些情况下，设计应尽量使SIS实际可测试，也就是说，至少通过电磁阀。在这种情况下，设计中可以包含电磁阀周围的某种旁路形式，利用这种旁路常用的报警或者规程控制。

对带测试和/或旁路设施的要求



对强制输入\输出的限制

- 作为以下内容的一部分，不应对PE SIS使用强制的输入和输出：

——应用软件；

——操作过程；

------维护，以下所说的除外。

- SIS不停机就不允许强制输入和输出，除非增补规程和访问保密机制。如合适，任何这种强制都应发出通告或发出一个报警。

10 SIS的现场验收测试要求

SAT, 安全确认

目　的

目的

- 审查和测试安装和调试好的安全仪表系统
- 确认相关的SIF实现了安全要求规范中所声明的那些要求。

制定验收测试计划

检验测试计划

- 检验测试应包括从传感器到最终单元的完整SIF。
  - 可以分开完成，但所有部件必须都进行测试
- 可以在线或离线测试
- 验收测试应包括检查和预防性维护活动
  - 目标是使设备恢复“如新”的状态

制定确认验收计划

1. 定义针对安全要求规范的确认活动
2. 定义针对过程及其相关设备的所有相关操作模式的确认活动，包括：
   --使用准备，包括设置和调整；
   --启动、自动、手动、半自动、稳定运行状态；
   --重置、停机、维护；
   --合理可预见的异常工况，例如通过风险分析阶段识别出的那些异常工况；
3. 确认所使用的规程、措施和技术

制定确认验收计划

— 进行这些活动的时间表；

— 负责这些活动的人员、部门和组织，以及确认活动的独

立性水平；

— 执行确认活动所依据的引用信息（如因果图）。

确认活动的例子包括回路测试、校准规程和应用软件仿真。

编制安全应用软件
附加确认验收计划

编制安全应用软件的附加确认验收计划

计划内容包括：

a) 在开始调试运行之前需在每种过程操作模式下进行确认的安全软件的标识；

b) 有关确认的技术策略的信息，包括：

— 手动和自动技术；

— 静态和动态技术；

— 分析和统计技术；

c) 根据b)，为证实每个安全仪表功能符合规定的软件安全仪表功能（见12.2）要求和规定的软件安全完整性要求（见12.2），应使用的措施（技术）和规程。

编制安全应用软件附加确认验收计划

d) 进行确认活动所要求的环境（例如，为了测试，要求包
括校正工具和设备）。
e) 为完成软件确认所需的通过/失败准则，包括：
— 要求的过程和操作员输入信号以及它们的顺序和值；
— 预期的输出信号以及它们的顺序和值；
— 其他验收准则，如存储器用法、定时和值的容差；
f) 评价确认结果（特别是失败）的策略和规程。

注意测量精度

测量精度的把握

- 在要求把测量精度作为确认的一部分时，应对照一个可追溯到某个标准的规范，把用于此功能的仪表校准到适合该应用的某个不确定度范围内。如果这种校准不可行，则应使用一种替代方法并文档化。

SIS确认验收

验收内容

应根据SIS确认验收计划对SIS及其相关的SIF进行确认。

验收内容

—在正常和异常操作模式（如启动和停机）下SIS都能按SRS要求履行其智能；

— 证实基本过程控制系统和连接的其他系统的相互作用，不会对SIS的正确运行产生不利的影响；

— SIS能同基本过程控制系统或任何其他系统或网络正确地通信；

验收内容

— 传感器、逻辑解算器和最终元件，包括所有冗余通道，按SRS运行；
注：如果已按标准对逻辑解算器进行过工厂验收测试（FAT），也可以把FAT认作是对逻辑解算器的确认。
— SIS文档应与被安装的系统相符；
— 证实能按照规定对无效过程变量值（如超出范围）执行安全仪表功能；
— 建立正确的停机顺序；
— 安全仪表系统提供正确的通告和运行显示；
— 安全仪表系统中包含的计算是准确的；

验收内容

— 按安全要求规范中定义的那样执行安全仪表系统的复位功能；
— 旁路功能正确运转；
— 启动超驰正确操作；
— 手动停机系统正确运转；
— 在维护规程中已编入检验测试间隔；
— 按要求的那样执行诊断报警功能；
— 证实在中断共用设施供应（如电、空气和液压）时，能按要求的那样运转安全仪表系统，并证实当恢复供应时，安全仪表系统可返回到所期望的状态；
— 证实已达到安全要求规范中所规定的EMC抗扰性。

附加说明

如果SIS已通过FAT，那么在验收过程中，这可能应被考虑。

确认组应审查FAT的结果，以确保成功地测试了所有的应用软件，并且纠正了FAT过程中发现的所有问题。

附加要求

在最终工厂验收时，不必重复测试应用软件，这要求满足下列所有条件：

— 预先考虑过这种方法，并且在工厂验收计划编制中包含此方法；

— 在FAT期间，应用软件已被验证是满足安全要求规范的；

— 验证应用软件版本与在FAT时测试的版本相同。

应用要求

然而，确保不存在装运/存放/吊装损伤、确保所有传感器和最终元件已被正确地连接到逻辑解算器上、确保正确执行了仪表安全功能，以及确保操作员接口能提供必要的信息是非常重要的。因为逻辑解算器和最终元件的分离测试并不等于整体的端对端检验测试，所以为了声明SIS确认，强烈推荐进行一次等效的检验测试。

软件确认验收

软件确认验收

软件确认应显示出所有规定的软件安全要求都能被正确执行，并且在SIS的故障工况下及降级操作模式下，或者在执行规范中未定义的软件功能性期间，软件都不会危害安全要求。应提供确认活动的信息。

完成SIS确认结果文档

SIS确认结果文档内容

应包括：

— 所使用的SIS确认计划编制的版本；

— 被测试（或分析）的安全仪表功能，及其在SIS确认计划编制过程中被标识要求的特定引用；

— 使用的工具和设备，及其校准数据；

— 每次测试的结果；

— 使用的测试规范的版本

SIS确认结果文档内容

还包括：

— 集成测试的验收准则；

— 被测试SIS硬件和软件的版本；

— 预期的和实际的结果之间的任何差异；

— 在出现差异的情况下，对差异所作的分析，以及对是否继续进行测试或是发布一个变更请求而作出的决定。

确认失败的处理

确认失败的处理

当预期的和实际的结果之间出现差异时，应把所作的分析和对是否继续进行测试或是发布一个变更请求并返回到开发生命周期的较早部分所作的决定当作安全确认的部分结果提供出来。

SIS确认验收后的活动

SIS确认验收后的活动

在SIS确认之后以及所存在的风险被识别出来之前，应进行下列活动：

—应返回所有旁路功能（如：对PE逻辑解算器和PE传感器的强制、禁止报警）的正常位置；

—应按过程起动要求和规程设置所有的过程隔离阀；

—应移除所有的测试材料（如流体）；

—应移除所有的强制，如适用还应消除所有强制使能。

青岛劳帕安全技术咨询有限公司

核心业务

- 安全仪表系统功能评估：安全完整性等级SIL定级、验证/验算
- 过程工艺危害分析 **HAZOP**
- 培训：安全完整性等级SIL定级、验证/验算、HAZOP等培训

微信扫一扫

微信号 :**qd13184148810**

电话：13184148810

QQ:1930712371

邮箱：qingdaolopa@163.com

网址：www.qingdaolopa.com