Evaluation Method for SIS Hardware Error Possibility

陈高翔[1]　冯冬芹[1,2]

（浙江中控技术有限公司[1]，浙江杭州 310053；浙江大学先进控制研究所[2]，浙江杭州 310027）

摘　要：首先介绍了安全仪表系统在实际应用中的需求以及安全仪表系统的硬件失效概率评估的必要性。然后，在研究了硬件失效概率的评估方法后，分析了低要求模式下 SIS 系统在各种表决组的物理块图和可靠性块图。最后，通过一个范例的计算详细介绍了具体结构下 SIS 系统的硬件失效概率评估方法。

关键词：安全仪表系统　安全完整性等级　平均失效概率　低要求操作模式　表决

Abstract: Firstly，this paper brings out the requirement of the Safety Instrument System in practical application and introduces the necessity of the PFD evaluation for SIS. After studying the evaluation method for PFD, this paper analyzes physical block diagram and reliability block diagram of a lot of kinds vote group for SIS in low demand mode of operation. Finally, an example is used to introduce the procedure of PFD evaluation.

Keywords: SIS　SIL　PFD　Low demand mode of operation　Vote

0　引言

由于当今工业的高度发展，整个工业过程是在一种高强度、高度自控的环境下进行，尤其是对于天然气、石油化工、化工及电力行业来说，由于企业生产的性质所决定，所处的生产环境是具有爆炸危险性的。这样，设备、人身及生产过程的安全可靠性就成为重要的议题。而传统的 DCS、PLC 系统等控制手段在这方面表现出的薄弱性也就越来越明显，这显然不能满足石油化工等危险场合的生产工艺要求。

在传统意义上，安全保护指的是额外的系统或设备用于保护在危险生产区域的工作人员免受伤害或死亡。然而今天，安全解决措施已经不仅仅是保证人生安全，并且生产厂商需要不断提升生产装置的运行性能，以便实现公司的利益最大化。生产厂商已经逐渐认识到智能集成的安全解决措施能够直接影响他们的账本底线。

随着 IEC 61508、IEC 61511 和 ISA-84 等功能安全国际标准的正式发布，生产厂商和用户越来越关注生产装置的功能安全要求，纷纷对危险和风险进行严格的分析，并开发、验证和应用已经经过功能安全认证的安全仪表系统（SIS）。SIS 是对石油化工生产装置可能发生的危险或不采取措施将继续恶化的状态进行及时响应和保护，使生产装置进入一个预定义的安全停车工况，从而使危险降低到可以接受的最低程度，以保证人员、设备、生产和装置的安全。为了提高企业的经济效益，安全平稳、长周期地连续生产是至关重要的，这就需要一种高度可靠的安全保护手段，SIS 系统因此应运而生。SIS 系统是适用于高温、高压、易燃、易爆等连续性生产装置的安全保护系统。

为了保证生产安全运行，根据具体要求对安全保护控制系统的设计选型工作是非常重要的。在安全系统的设计中，安全完整性等级 SIL 是设计的标准，应根据生产装置的 SIL 等级选择合适的安全系统技术和配置方式。SIL 等级可用于简化和理论化系统结构中各部分的安全要求，并使

其定量化。IEC 61508 定义了 4 个安全度等级及相应于每个等级的两个定量安全要求，包括对系统按照要求切换到安全功能的目标故障率要求和对系统连续操作的目标故障率要求。本文将着重介绍各种系统结构下的对系统按照要求切换到安全功能的目标故障率要求的计算方法及示例。

1 硬件失效概率评估方法综述

SIS 系统结构如图 1 所示。

SIS 安全功能在要求时的平均失效概率，是通过计算和组合提供安全功能的所有子系统在要求时的平均失效概率确定的。SIS 在要求时的平均失效概率如公式（1）所示。

$$PFD_{SYS}=PFD_S+ PFD_L +PFD_{FE} \quad (1)$$

式中：

PFD_{SYS}为SIS的安全功能在要求时的平均失效概率；

PFD_S为传感器子系统在要求时的平均失效概率；

PFD_L为逻辑子系统在要求时的平均失效概率；

PFD_{FE}为最终元件子系统在要求时的平均失效概率。

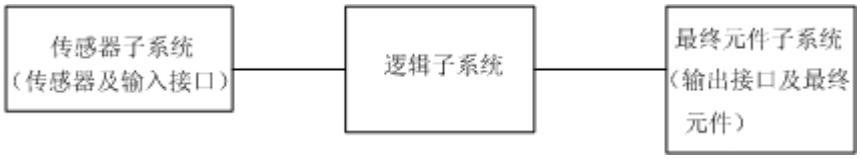

图 1 SIS 系统结构

为了确定每一个子系统在要求时的平均失效概率，应在子系统中：

① 画出表示传感器子系统（输入）各部件、逻辑子系统各部件、最终元件子系统（输出）各部件的块图。例如，传感器子系统的部件可能是传感器、绝缘电路、输入调节电路；逻辑子系统部件可能是处理器和扫描设备;最终元件子系统部件可能是输出调节电路、屏蔽电路及执行器。将每一个子系统描绘成 1oo1、1oo2、2oo2、1oo2D、2oo3 表决组。

② 对于每一个子系统中的表决组要从 IEC61508 第六部分表 B.2 至 B.5 相关的表中选择：

结构（例如 2oo3）；

每个通道的诊断覆盖率（例如 60%）；

每个通道的失效率（每小时）λ，（例如 5.0E-06）；

表决组中通道之间相互作用的共同原因失效的β-系数， β 和βD，（例如分别为 2%和 1%）。

③ 如果安全功能依赖于传感器或执行器的多个表决组，传感器或最终元件子系统在要求时的组合平均失效概率PFD_S或PFD_{FE}已在下列式子中给出，其中PFD_{Gi}、PFD_{Gj}分别为传感器与最终元件的每个表决组在要求时的平均失效概率：

$$PFD_S=\sum PFD_{Gi} \quad (2)$$

$$PFD_{FE}=\sum PFD_{Gj} \quad (3)$$

2 SIS 系统结构和可靠性分析

对于 SIS 系统中每个通道的未检测故障，必须通过 SIS 系统的自诊断程序或外部的人工测试来排除，才能保证 SIS 的可靠性。采用故障-安全方式，虽然能有效防止 SIS 系统的未检测故障的发生，但仪表接线松动和电磁阀、测量仪表等故障都会引起 SIS 误动作及装置误停车。

如何有效消除 ESD 系统中的显性故障和隐性故障对生产装置正常运行的影响？对于现场检

测仪表和执行单元，目前还无十分有效的诊断措施，但可从逻辑上采取一些措施：

① 采用“二选一”表决组方式，两个通道中任一个触发，SIS 系统就联锁动作，可靠性较高，但任一通道故障均可引起误停车。

② 采用“二选二”表决组方式，当两个通道同时触发，SIS 系统才联锁动作，一个通道有故障不会产生停车，误停车率小，可用性高。但“二选二”方式也存在缺陷，若系统中的任一通道存在未检测故障，则可能引起危险情况的发生，可靠性低。

③ 采用“三选二”表决组方式。仅当 3 个通道中任意两个同时触发，SIS 系统联锁动作。其中任一个通道出现故障不会导致误停车，也不会导致危险发生。

由上述分析可知：单独的“二选一”、“二选二”逻辑方式不能兼顾系统的可靠性和可用性。“三选二”逻辑表决方式能有效防止检测故障和未检测故障的发生，兼顾系统的可靠性和可用性。因为在计算平均失效概率的过程中，将使用很多参数，所以将这些参数先简单介绍一下。

在公式（4）～公式（7）中：

λ 为子系统中一个通道的失效率；

λ_D为子系统中通道的危险失效率；

λ_{DU}为未检测到的子系统中通道每小时的危险失效率；

λ_{DD}为检测到的子系统中通道每小时的危险失效率；

λ_{SD}为子系统中被检测到的通道每小时的安全失效率；

t_{CE}为 1oo1、1oo2、2oo2、1oo2D、2oo3 结构中通道的等效平均停止工作时间；

t_{GE}为 1oo2、2oo3 结构中表决组的等效平均停止工作时间；

t_{CE}’ 为 1oo2D结构中通道的等效平均停止工作时间；

t_{GE}’ 为 1oo2D结构中表决组的等效平均停止工作时间；

T_1为检验测试时间间隔；

MTTR 为平均恢复时间；

DC 为诊断覆盖率；

PFD 为单通道在要求时的平均失效概率；

PFD_G为表决通道组在要求时的平均失效概率；

B 为具有共同原因的、没有被检测到的失效分数；

β_D为具有共同原因的、已被诊断测试检测到的失效分数。

2.1 一选一（1oo1）

这种结构包括一个单通道，当产生一次要求时，任何危险失效就会导致一个安全功能失效。

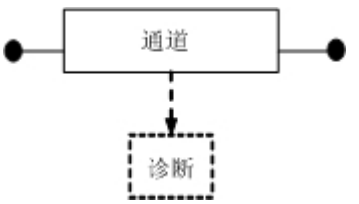

图 2 1oo1 物理块图

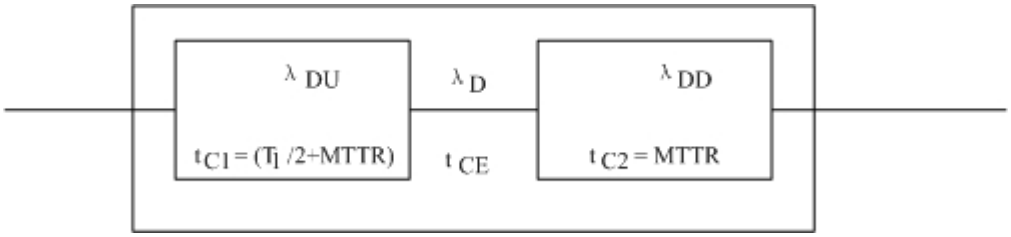

图 3　1oo1 可靠性块图

图 2 和图 3 包括了有关的块图，通道的危险失效率为

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \lambda /2 \quad (4)$$

如图 3 所示，通道可以被认为由两部分组成，其中一个具有由未被检测到的失效导致的危险失效率 λ_{DU}，另一部分具有由已被检测到的失效导致的危险失效率 λ_{DD}，通道的等效平均停止工作时间 t_{CE}，等于两部分各自的停止工作时间t_{c1}和t_{c2}相加，各部分所占比例对通道失效率的影响如下：

$$t_{CE} = \lambda_{DU}/\lambda_D \times (T1/2+MTTR) + \lambda_{DD}/\lambda_D \times MTTR \quad (5)$$

对于每种结构，已被检测和未被检测到的危险失效率

$$\lambda_{DU} = \lambda /2 \times (1-DC) \quad (6)$$

$$\lambda_{DD} = \lambda /2 \times DC \quad (7)$$

对于一个具有由危险失效而导致关闭时间为t_{GE}的通道：

$$PFD = \lambda_D \times t_{CE} \quad (8)$$

因此，对于 1oo1 结构，在要求时的平均失效概率如下：

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) \times t_{CE} \quad (9)$$

2.2　二选一（1oo2）

此结构由两个并联的通道构成，无论哪一个通道都能处理安全功能。因此，如果两个通道都存在危险失效，则在要求时某个安全功能失效。假设任何诊断测试仅报告发现故障，但并不改变任何输出状态或输出表决。

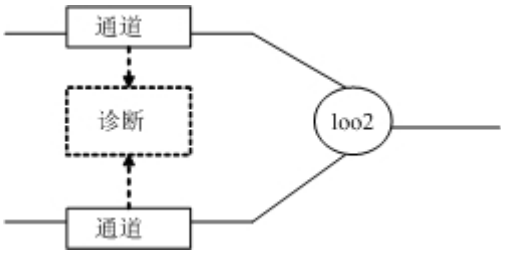

图 4　1oo2 物理块图

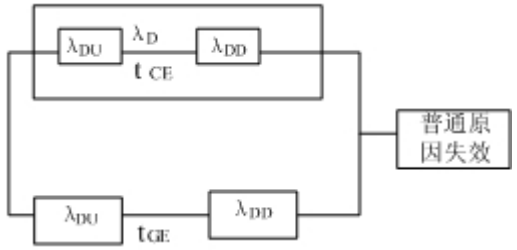

图 5　1oo2 可靠性块图

图 4 和图 5 中包含了相关的块图。t_{CE}的值如公式（5）所示，但是现在有需计算系统等效停止工作时间t_{GE}，表示如下：

$$t_{GE} = \lambda_{DU}/\lambda_D \times (T1/3+MTTR) + \lambda_{DD}/\lambda_D \times MTTR \quad (10)$$

此结构在要求时的平均失效概率为：

$$PFD_G = 2\times((1-\beta) \times \lambda_{DU} + (1-\beta D)\ \lambda_{DD})2\times t_{CE}\times t_{GE} + \beta_D \times \lambda_{DD} * MTTR + \beta \times \lambda_{DU} \times (T1/2+MTTR) \quad (11)$$

2.3　二选二（2oo2）

此结构由并联的两个通道构成，因此，在发生安全功能之间两个通道都要求安全功能。假设任何诊断测试仅报告发现故障，并不改变任何输出状态或输出状态。

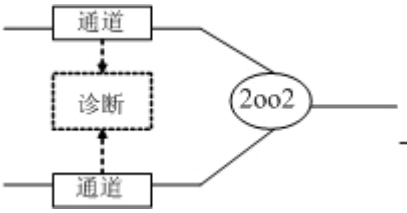

图 6　2oo2 物理块图

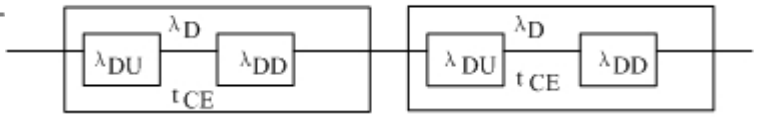

图 7　2oo2 可靠性块图

图 6 与图 7 包含了相关的块图。tCE 的值如公式（5）所示，此结构在要求时的平均失效概率如下：

$$PFD_G = 2 \times \lambda_D \times t_{CE} \quad (12)$$

2.4　带诊断的二选一（1oo2D）

此结构中由并联的两个通道构成，正常工作期间，在发生安全功能之间，两个通道都要求安全功能。此外，如果任一通道中诊断测试检测到一个故障，则将采用输出表决，因此整个输出状态按照另一通道给出的输出状态。如果诊断测试在两个通道同时检测到故障，或者检测到两个通道间存在的差异时，输出则转到安全状态。为了检测两个通道间的差异，通过一种与另一通道无关的方法，无论其中哪个通道都能确定另一通道的状态。

每个通道中被检测的安全失效率如下：

$$\lambda_{SD} = \lambda / 2 \times DC \quad (13)$$

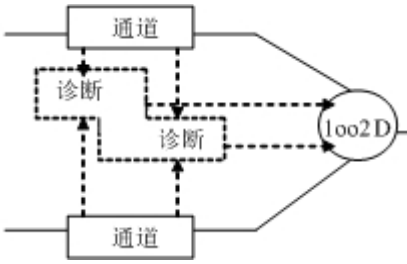

图 8　1oo2D 物理块图

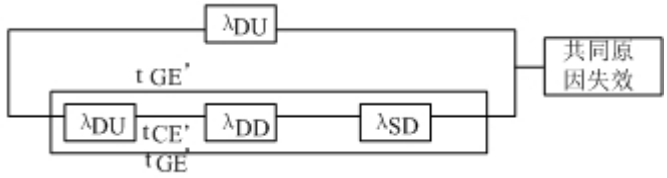

图 9　1oo2D 可靠性块图

图 8 和图 9 包含相关的块图，它们的平均停止工作时间表示为t_{CE}’与 t_{GE}’，其表达式如下：

$$t_{CE}' = [\lambda_{DU} \times (T1/2+MTTR) + (\lambda_{DD} + \lambda_{SD}) \times MTTR] / (\lambda_{DU} + \lambda_{DD} + \lambda_{SD}) \quad (14)$$

$$t_{GE}' = [\lambda_{DU} \times (T1/3+MTTR) + (\lambda_{DD} + \lambda_{SD}) \times MTTR] / (\lambda_{DU} + \lambda_{DD} + \lambda_{SD}) \quad (15)$$

结构在要求时的平均失效概率如下：

$$PFD_G = 2 \times (1-\beta) \times \lambda_{DU} \times ((1-\beta) \times \lambda_{DU} + (1-\beta_D) \times \lambda_{DD} + \lambda_{SD}) \times t_{CE}' \times t_{GE}' + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times (T1/2+MTTR) \quad (16)$$

2.5　三选二（2oo3）

此结构由 3 个并联通道构成，其输出信号具有多数表决安排，这样，如果仅其中一个通道的输出与其它两个通道的输出状态不同时，输出状态不会因此而改变。假设任何诊断测试只报告发现故障，不改变任何输出状态或输出表决。

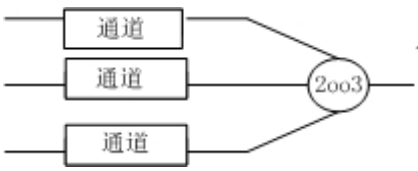

图 10　2oo3 物理块图

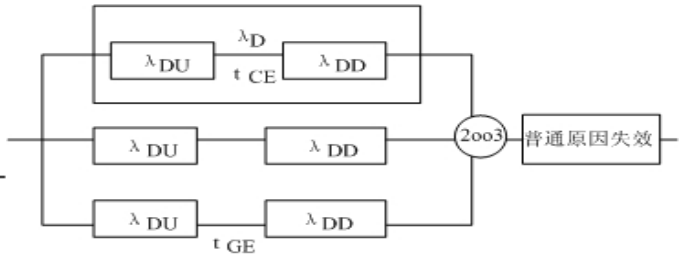

图 11　2oo3 可靠性块图

图 10 和图 11 包含了相关的块图。t_{CE}的值如公式（5）所示， t_{GE}的值如公式（10）所示。结构在要求时的平均失效概率为

$$PFD_G=6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})2\times t_{CE}*t_{GE}+\beta_D\times\lambda_{DD}\times MTTR+\beta\times\lambda_{DU}\times(T1/2+MTTR) \quad (17)$$

3　低要求操作模式的范例

考虑需求一个 SIL2 系统的安全功能。假设按前面的做法对系统结构的初始评价是，针对 1 组 3 个模拟压力传感器结构为表决 2oo3。逻辑子系统是配置为冗余 1oo2D 的 SIS，用于驱动 1 个停机阀和 1 个通风阀，为了达到安全功能，需要操作通风阀和停机阀，在图 12 中显示了该系统的结构。初始评估时假设检验测试时间间隔为一年。

从表 1 至表 3 中导出下列公式：

对于传感器子系统　　$PFD_S = 2.3\times10^{-4}$

对于逻辑子系统　　$PFD_L = 4.8\times10^{-6}$

对于最终元件子系统 $PFD_{FE} = 4.4\times10^{-4}+8.8\times10^{-4}=1.3\times10^{-2}$

因此，对于安全功能

$$PFD_{SYS} = 2.3\times10^{-3}+4.8\times10^{-6}+1.3\times10^{-2}=1.3\times10^{-2}$$

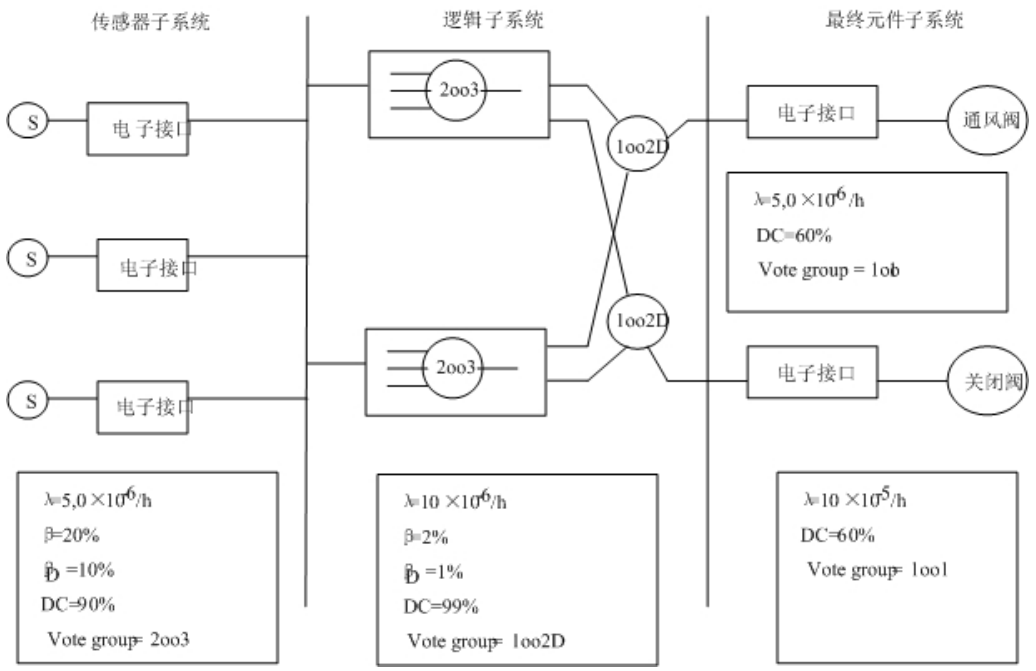

图 12　2oo3 可靠性块图

表 1　低要求模式示例中传感器子系统在要求时的平均失效概率
（检验测试时间间隔为 1 年，MTTR 为 8 小时）

结构	DC	λ=1.0E-05		
		β=2% βD =1%	β=10% βD =5%	β=20% βD =10%
2oo3	0%	6.8E-04	1.5E-03	2.5E-03
	60%	1.6E-04	5.1E-04	9.4E-04
	90%	2.7E-05	1.2E-04	2.3E-04
	99%	2.5E-06	1.2E-05	2.4E-05
注：此表是 IEC61508 第六部分表 B.3 的摘要				

表 2　低要求操作模式实例中的逻辑子系统在要求时的平均失效概率
（检验测试时间间隔为 1 年，MTTR 为 8 小时）

结构	DC	λ=1.0E-05		
		β=2% βD =1%	β=10% βD =5%	β=20% βD =10%
1oo2D	0%	1.1E-03	2.7E-03	4.8E-03
	60%	2.0E-04	9.0E-04	1.8E-03
	90%	4.5E-05	2.2E-04	4.4E-04
	99%	4.8E-06	2.4E-05	4.8E-05
注：此表是 IEC61508 第六部分表 B.3 的摘要				

表 3　低要求操作模式示例中最终元件子系统在要求时得平均失效概率
（检验测试时间间隔为 1 年，MTTR 为 8 小时）

结构	DC	λ=5.0E-06	λ=1.0E-05
1oo1	0%	1.1E-02	2.2E-02
	60%	4.4E-03	8.8E-03
	90%	1.1E-04	2.2E-03
	99%	1.3E-04	2.6E-04
注：此表是 IEC61508 第六部分表 B.3 的摘要			

由以上结构计算而得的 SIS 只能满足 SIL1 的要求，所以为了改进系统，使其更好地适应 SIL2 的需求，可以采用以下方法进行改进：

① 将验证检测的时间间隔改为 6 个月

对于传感器子系统　　$PFD_S = 1.1\times10^{-4}$

对于逻辑子系统　　$PFD_L = 2.6\times10^{-6}$

对于最终元件子系统 $PFD_{FE} = 2.2\times10^{-4}+4,4\times10^{-4}=6.6\times10^{-3}$

因此，对于安全功能 $PFD_{SYS} = 6.7\times10^{-3}$

② 将 1oo1 停机阀(其输出设备的可靠性较低)改为 1oo2（假设 β 为 10%，βD 值为 5%）

对于传感器子系统　　$PFD_S = 2.3\times10^{-4}$

对于逻辑子系统　　$PFD_L = 4.8\times10^{-6}$

对于最终元件子系统 $PFD_{FE} = 4.4\times10^{-4}+9.7\times10^{-4}=5.4\times10^{-3}$

因此，对于安全功能 $PFD_{SYS} = 5.6\times10^{-3}$

由此，对于此 SIS 系统实现的安全功能的 SIL 等级提高到 SIL2。

4 结束语

众多 SIS 系统应用实例证明，SIS 系统在避免工业灾难、减少工业事故损失方面起到了积极和重要的作用，它为工业过程中要求最大安全与连续生产的关键控制提供了一种最佳选择。在设置安全系统时，既要满足工业过程安全度要求，又要保证可靠性。因此，必须先对具体的工业过程进行安全度的评价，再根据具体工艺环境的要求设定满足于安全要求的安全仪表系统。

硬件失效概率评估方法从传感器子系统、逻辑子系统和最终元件子系统的表决组类型入手，根据子系统结构、每个通道的诊断覆盖率、每个通道的失效率、表决组中通道之间相互作用的共同原因失效的β-系数，计算出各个子系统的平均失效概率，从而得出整个 SIS 系统的平均失效概率。此方法可以方便地应用于 SIS 系统的设计阶段，从而满足工艺环境对安全的要求。

参考文献

1 IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related system[S], 1998.

2 IEC 61511: Functional safety - Safety instrumented systems for the process industry sector[S], 2002.

3 ANSI/ISA－S84.01－1996: Application of Safety Instrumented Systems for the Process Industries[S], 1997.

4 HG/T 20511-2000: 信号报警、安全连锁系统设计规定[S]，2001.

5 SHB-Z06-1999: 石油化工紧急停车及安全连锁系统设计导则，1999.

6 SH/T3018-2003: 石油化工安全仪表系统设计规范，2003.