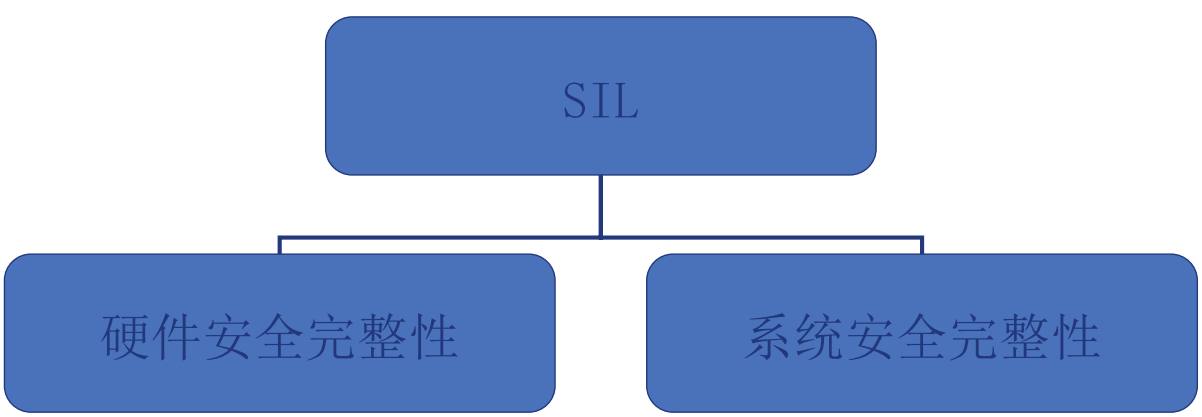
硬件安全完整性要求

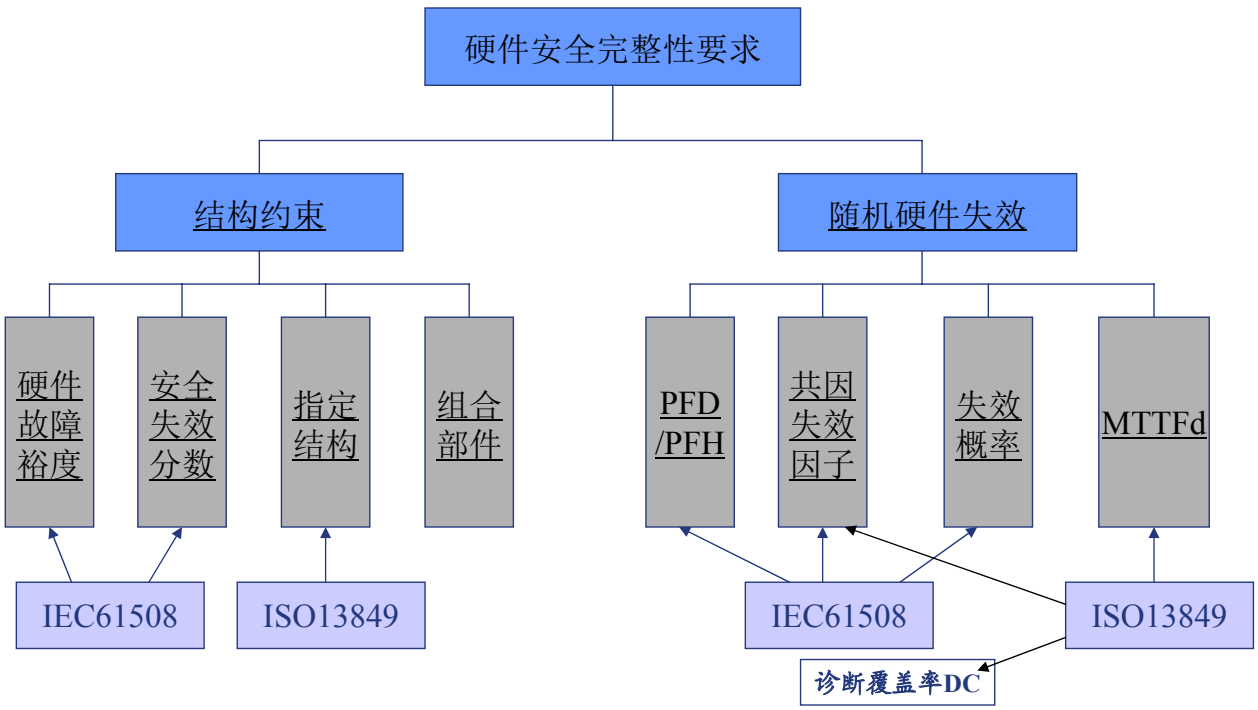
机械工业仪器仪表综合技术经济研究所 副总工程师
全国工业过程测量与控制标准化技术委员会 系统及功能安全分技术委员会
（SAC/TC124/SC10）副主任委员
史学玲教授

安全完整性

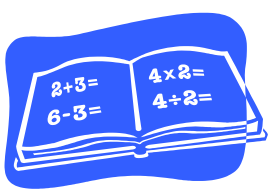


机械工业仪器仪表综合技术经济研究所
中国功能安全中心 FSCHINA

硬件安全完整性要求



结构约束



结构约束—IEC61508

硬件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：

◆ 硬件故障裕度N意味着N+1个故障会导致安全功能的丧失，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；

◆ 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；

◆ 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。

◆ 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。

硬件故障裕度（HFT）

HFT与冗余

HFT = 0　单通道系统

HFT = 1　冗余系统

HFT = 2　三重冗余

1oo3	三个通道	HFT=2
2oo3	→	HFT=1
3oo3		HFT=0

A类安全相关子系统的结构约束

满足下列条件的子系统可视为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，或由电阻、电容放大器等构成的简单电子模块。

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

B类安全相关子系统的结构约束

满足下列条件的子系统可视为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。

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

MooN表决结构

定义：

在一些工作并联配置中，需要n中的m个单元能工作，以使系统能起作用。这称为n中取m（或m/n）并联冗余.

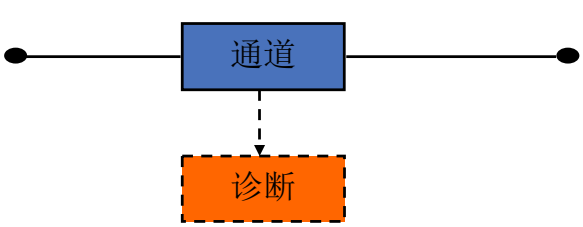
常用的表决结构：

1oo1, 1oo2, 2oo2, 2oo3, 1oo1D, 1oo2D

MooN表决结构

1oo1

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



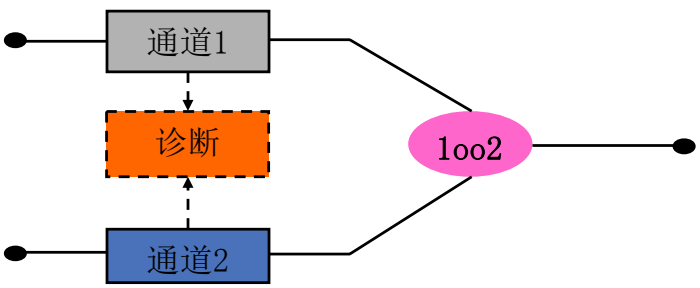
图V1　1oo1物理块图

机械工业仪器仪表综合技术经济研究所 中国功能安全中心 FSCHINA

MooN表决结构

1oo2

此结构由两个并联的通道构成，无论那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。

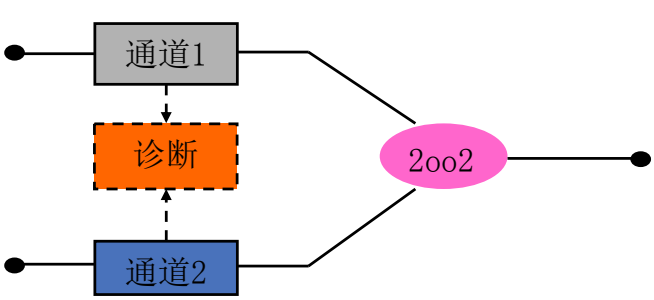


图V2　1oo2物理块图

MooN表决结构

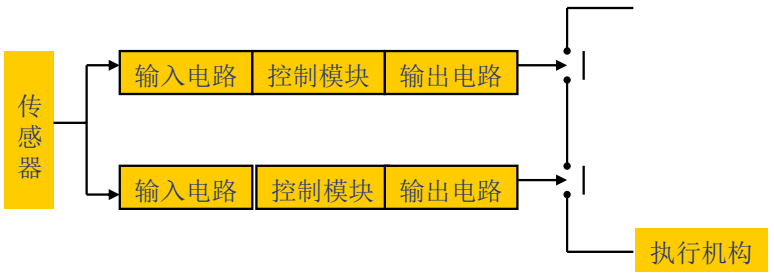
2oo2

此结构由并联的两个通道构成，因此，安全功能要求两个通道都工作。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表决。

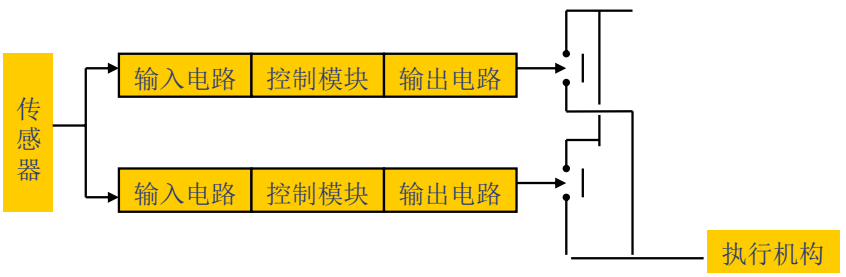


图V3　2oo2物理块图

MooN表决结构



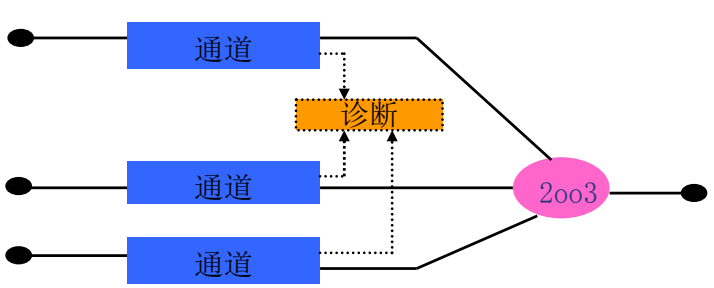
- 2oo2 or 1oo2 ?



MooN表决结构

2oo3

此结构由三个并联通道构成，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者输出表决。

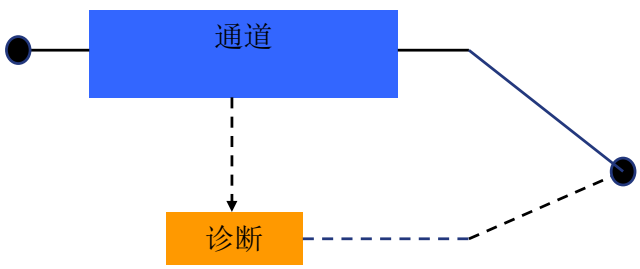


图V4　2oo3物理块图

MooN表决结构

1oo1D

这种结构包括一个带有诊断能力的功能单通道和一个诊断通道，两者均能将输出转到安全状态。



图V5　1oo1D物理块图

与1oo1的区别和联系？

MooN表决结构

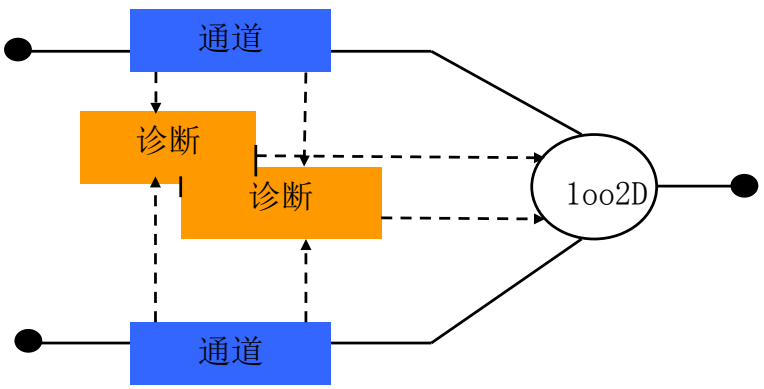
1oo2D

此结构中由并联的两个通道构成，正常工作期间，两个通道都执行安全功能。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，因此整个输出状态则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，无论其中那个通道都能确定另一通道的状态。

MooN表决结构

1oo2D



图V6　1oo2D物理块图

MooN表决结构

安全PLC结构的变化

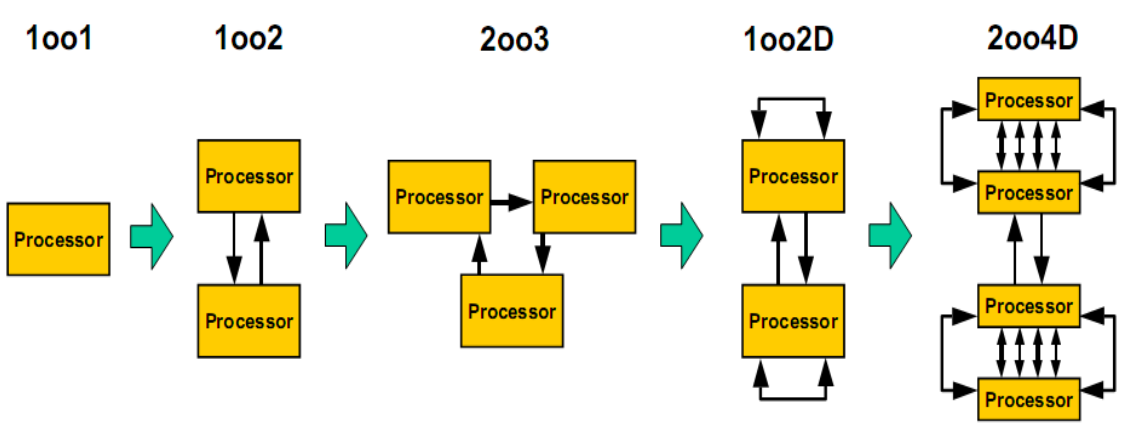
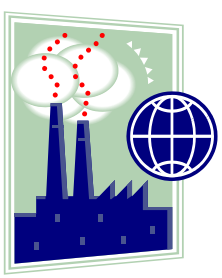


Figure 1　Evolution of safety PLC architectures

安全失效分数（SFF）



安全失效分数（SFF）

定义：

实际意义上的安全失效率占总失效率的百分比

$$SFF = \frac{\Sigma \lambda_{DD} + \Sigma \lambda_{S}}{\Sigma \lambda}$$

其中：λ_{DD} —— 检测到的危险失效的概率；

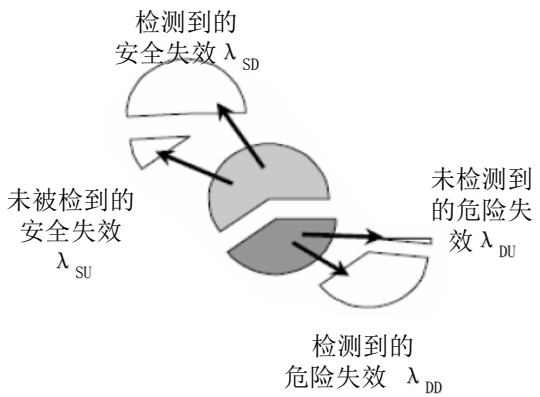
λ_{S} —— 安全失效的概率。

λ —— 总的失效概率。

安全失效分数（SFF）

把每个失效率分为“检测出”和“未被检出”（通过在线测试）

$$\lambda^{S} = \lambda^{SD} + \lambda^{SU}$$



$$\lambda^{D} = \lambda^{DD} + \lambda^{DU}$$

安全失效分数（SFF）

- 安全失效分数体现的是子系统在线诊断的能力
- 可同时提高可用性与安全性
- 其优点取决于具体的系统结构

用法：

与硬件故障裕度（HFT）一起，用来验证硬件结构约束的安全完整性。

机械工业仪器仪表综合技术经济研究所
中国功能安全中心 FSCHINA

安全失效分数（SFF）

危险失效分为检测到的危险失效λ_{DD}与未检测到的危险失效 λ_{DU}。检测到的危险失效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。

$$\lambda_{DD} = \lambda_D \cdot DC^d$$

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

安全失效分数（SFF）

传感器的诊断：

单个传感器		60%
二个传感器		80%
多个传感器	2oo3，2oo4	90%

机械工业仪器仪表综合技术经济研究所 中国功能安全中心 FSCHINA

安全失效分数（SFF）

SFF计算示例

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

例：

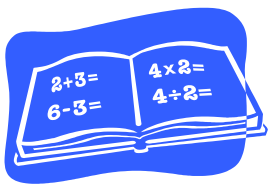
单元：FIT（10E-09）

器件	λ	DC	λ_S	λ_{DD}	λ_{DU}	$\lambda_S+\lambda_{DD}$
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%

诊断覆盖率

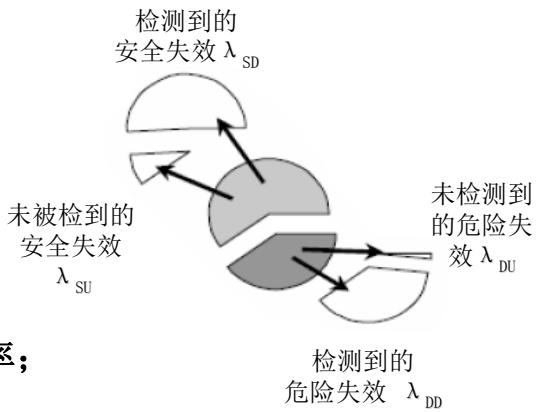


诊断覆盖率DC

定义：

进行自动诊断测试而导致的硬件危险失效概率的降低部分。

$$DC = \frac{\Sigma \lambda_{DD}}{\Sigma \lambda_{D}}$$



式中：

DC —— 诊断覆盖率；

λ_{DD} —— 检测到的危险失效的概率；

λ_{D} —— 危险失效的概率。

诊断覆盖率DC

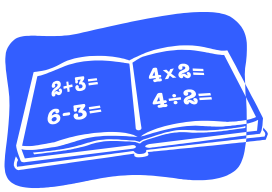
用法：

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

设备的诊断覆盖率计算：

- 设备研发制造企业的工作；
- 设计和工程单位可直接向产品供应商索取

提高诊断覆盖率的措施



提高诊断覆盖率的措施

为达到诊断覆盖率的相应级别（见附录C），表A.1给出了为控制硬件失效而由技术和措施检测出的故障和失效的要求。表A.2-表A.15支持表A.1的要求，为诊断测试推荐了技术和措施，并推荐了使用这些技术和措施可实现的最高的诊断覆盖率等级。这些测试可以连续地或定期地进行。这些表并不取代7.4的任何要求。表A.2~表A.15并不详尽，当然还可使用其他技术和措施，只要提供相应的证据，保证支持所声明的诊断覆盖率。

1：GB/T20438.7的附录A给出了这些表中所有技术和措施的概述。表A.2～表A.15的第二列给出了要求所在的条款。

2：诊断覆盖率的低、中和高3级分别定量为60%、90%和99%。

机械工业仪器仪表综合技术经济研究所
中国功能安全中心 FSCHINA

表A.1 在操作过程中要检测或在推导安全失效分数中要分析的故障或失效

部件	见表	对所声明的诊断覆盖率或安全失效分数的要求		
		低（60%）	中（90%）	高（99%）
机电装置	A.2	未加电或断电 触点被熔接	未加电或断电 单个触点被熔接	未加电或断电 各触点被熔接 不可靠的导向触点（对于继电器，若按照EN50205或等同标准进行构建和测试，则不假定这种失效） 不可靠的开启（对于定位开关，若按照EN60947-5-1或等同标准构建和测试，则不假定这种失效）
分离硬件 数字I/O 模拟I/O 电源	A.3， A.7， A.9， A.11	固定故障（Stuck-at） 固定故障（Stuck-at） 固定故障（Stuck-at）	DC故障模型 DC故障模型 漂移和振动 DC故障模型 漂移和振动	DC故障模型 漂移和振动 DC故障模型 漂移和振动 DC故障模型 漂移和振动
总线 一般要求 内存管理单元 直接内存访问 总线仲裁 （见注1）	A.3 A.7 A.8	地址固定故障（Stuck-at） 数据或地址固定故障（Stuck-at） 无或连续访问 仲裁信号固定故障（Stuck-at）	超时 错误的地址解码 数据和地址的DC故障模型 访问时间错误 无或连续仲裁	超时 错误的地址解码 影响内存数据的所有故障 数据或地址错误 访问时间错误 无或连续或错误仲裁
CPU 寄存器，内部RAM 编码和执行，包括标记寄存器 地址计算 程序计数器，堆栈指针	A.4、 A.10	数据和地址固定故障（Stuck-at） 错误编码或不执行 固定故障（Stuck-at） 固定故障（Stuck-at）	数据和地址的DC故障模型 错误编码或错误执行 DC故障模型 DC故障模型	数据和地址的DC故障模型 内存单元的动态交叉 无寻址、错误寻址或多重寻址 未定义失效假设 未定义失效假设 DC故障模型

表A.1 在操作过程中要检测或在推导安全失效分数中要分析的故障或失效

部件	见表	对所声明的诊断覆盖率或安全失效分数的要求		
		低（60%）	中（90%）	高（99%）
中断处理	A.4	无或连续中断	无或连续中断 中断的交叉	无或连续中断 中断的交叉
不可变内存	A.5	数据和地址固定故障（Stuck-at）	数据和地址的DC故障模型	影响内存数据的所有故障
可变内存	A.6	数据和地址固定故障（Stuck-at）	数据和地址的DC故障模型 对于集成度不低于1Mbits的DRAM，软错误引起的信息改变	数据和地址的DC故障模型 内存单元的动态交叉 无寻址、错误寻址或多重寻址 对于集成度不低于1Mbits的DRAM，软错误引起的信息改变
时钟（石英）	A.12	分谐波或超谐波	分谐波或超谐波	分谐波或超谐波
通信和大容量存储器	A.13	错误的数据或地址 不传输	影响内存数据的所有故障 错误的数据或地址 错误的传输时间 错误的传输顺序	影响内存数据的所有故障 错误的数据或地址 错误的传输时间 错误的传输顺序
传感器	A.14	固定故障（Stuck-at）	DC故障模型 漂移和振动	DC故障模型 漂移和振动
最终元件	A.15	固定故障（Stuck-at）	DC故障模型 漂移和振动	DC故障模型 漂移和振动

注1：总线仲裁是一种决定哪个设备具有总线控制权的机制。
注2：固定故障（Stuck-at）是一种故障种类，可以用部件引脚的连续 “0”或“1”或 “on”来表示。
注3：“DC故障模型”（DC为直流）包括的失效模式有：固定故障（Stuck-at）、固定开故障（Stuck-open），开路或高阻抗输出以及信号线间的短路。

机械工业仪器仪表综合技术经济研究所 中国功能安全中心 FSCHINA

表A.2 电气子系统的诊断技术措施及覆盖率

诊断 技术/措施	见IEC61508.7	经考虑能达到的最大诊断 覆盖率	注
利用在线监视检测失效	A.1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
继电器触点监视	A.1.2	高	
比较器	A.1.3	高	若在安全导则中失效模式起支配作用，则高
多数表决器	A.1.4	高	依赖于表决质量
无功电流原理	A.1.5	低	仅对无需用连续控制来实现或维护EUC安全状态的E/E/PE安全相关系统有效
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.3 电子子系统诊断技术措施及覆盖率

诊断 技术/措施	见GB/TXXXX.7	经考虑能达到的最大诊断 覆盖率	注
利用在线监视检测失效	A.1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
比较器	A.1.3	高	若在安全导则中失效模式起支配作用，则高
多数表决器	A.1.4	高	依赖于表决质量
利用冗余硬件进行测试	A.2.1	中	依赖于失效检测的诊断覆盖率
动态原则	A.2.2	中	依赖于失效检测的诊断覆盖率
访问端口和边界扫描结构的标准测试	A.2.3	高	依赖于失效检测的诊断覆盖率
监视冗余	A.2.5	高	依赖于冗余和监视程度
带自动检验的硬件	A.2.6	高	依赖于测试的诊断覆盖率
模拟信号监视	A.2.7	低	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.4 处理单元诊断技术措施及覆盖率

诊断 技术/措施	见IEC61508.7	经考虑能达到的最大 诊断覆盖率	注
比较器	SIL1、SIL2、SIL3中采用， 双通道结构的比较器	高	依赖于比较的质量
多数表决器	A.1.4	高	依赖于表决的质量
利用软件进行自测试： 有限模式数（单通道）	SIL1中采用， 软件自检	低	
利用软件进行自测试： 漫步位（单通道）	A.3.2	中	
由硬件支持的自测试 （单通道）	SIL1中采用， 单通道结构的有硬件支持的软件自检	中	
编码处理（单通道）	SIL1、SIL2中采用， 可更正故障的硬件	高	
利用软件进行相互比较	SIL1、SIL2、SIL3中采用， 双通道结构的软件相互比较	高	依赖于比较的质量
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.5 不可变内存范围

诊断 技术/措施	见IEC61508.7	经考虑能达到的 最大诊断覆盖率	注
字保存多位冗余	A.4.1	中	
修正的校验和	A.4.2	低	
单字（8bit）的签名	SIL1、SIL2中采用， 具有一字冗余的块安全	中	签名的有效性依赖于与受保护的信息块长度有关的签名的宽度
双字（16bit）的签名	SIL3中采用， 具有多字冗余的块安全	高	签名的有效性依赖于与受保护的信息块长度有关的签名的宽度
块复制	SIL3中采用， 有复制块的块安全	高	
注1：本表不取换附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.6 可变内存范围

诊断 技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
“检测板”或“跨步”RAM测试法	A.5.1	低	
“漫步路径”RAM测试法	SIL1、SIL2中采用，通过测试模式检测静态或动态故障	中	
“galpat”或“透明galpat”RAM测试法	SIL3中采用，监视检查例如Galpat法	高	
“Abraham”RAM测试法	A.5.4	高	
RAM的奇偶位	A.5.5	低	
利用修改的海明码的RAM监视，或利用差错检测和纠错码（EDC）校验数据失效	A.5.6 SIL1、SIL2中采用，具有多位冗余的字保存	高	
带硬件或软件比较和读/写测试的双RAM	SIL3中采用，有复制块的块安全过程	高	

注1：本表不取代附录C的任何要求。
注2：附录C的要求与诊断覆盖率的确定有关。
注3：有关本表的一般注释，见表A.1前的正文。
注4：对于不经常读/写（例如组态过程）的RAM，若在每次读/写访问之后执行A.4.1～A.4.4的措施则可认为这些措施是有效的。

表A.7 I/O单元和接口(外部通信)

诊断 技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
测试模式	SIL1、SIL2、SIL3中采用，测试模式	高	
代码保护	SIL1、SIL2、SIL3中采用，代码安全	高	
多通道平行输出	SIL3中采用，多通道并行输出	高	仅当诊断测试间隔内数据流改变时才有效
监视输出	SIL3中采用，输出读回	高	仅当诊断测试间隔内数据流改变时才有效
输入比较/表决（1oo2，2oo3或更好的冗余）	SIL3中采用，多通道并行输入	高	仅当诊断测试间隔内数据流改变时有效

注1：本表不取代附录C的任何要求。
注2：附录C的要求与诊断覆盖率的确定有关。
注3：有关本表的一般注释，见表A.1前的正文。

表A.8 数据路径(内部通信)

诊断 技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
1位硬件冗余	A.7.1	低	
多位硬件冗余	A.7.2	中	
完全硬件冗余	A.7.3	高	
使用测试模式进行检查	A.7.4	高	仅对瞬时故障有效
传输冗余	A.7.5	高	
信息冗余	A.7.6	高	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.9 电源

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
使用安全断电或切换到备用电源单元的过压保护	A.8.1	低	应使用本表中的技术，也推荐使用其他技术
使用安全断电或切换到备用电源单元的电压控制（次级）	A.8.2	高	
带安全断电或切换到备用电源单元的断电	A.8.3	高	应使用本表中的技术，也推荐使用其他技术
无功电流原理	A.1.5	低	仅对断电有用
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.10 程序顺序(看门狗)

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
具有分离时基但无时间窗的看门狗	A.9.1	低	
具有分离时基和时间窗的看门狗	A.9.2	中	
程序顺序的逻辑监视	A.9.3	中	依赖于监视质量
程序顺序的时序和逻辑监视的组合	SIL1、SIL2、SIL3中采用，程序序列的时序和逻辑监视的组合	高	
具有在线检验的时序监视	A.9.5	中	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.11 通风和加热系统(若需要)

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
温度传感器	A.10.1	中	
风扇控制	A.10.2	中	
通过热保险丝启动安全断电	A.10.3	高	
来自温度传感器和条件报警的交错报文	A.10.4	高	
强制风冷的连接和状态指示	A.10.5	高	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.12 时钟

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
具有分离时基但无时间窗的看门狗	A.9.1	低	
具有分离时基和无时间窗的看门狗	A.9.2	高	依赖于时间窗的时间限制
程序顺序的逻辑监视	A.9.3	中	仅当外部瞬时事件影响逻辑程序流时才对时钟失效有效
时序和逻辑监视	SIL1、SIL2、SIL3中采用，具备独立时钟基准的看门狗	高	
具有在线检验的时序监视	A.9.5	中	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.13 通信和大容量存储器

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
E/E/PE安全相关系统和过程之间的信息交换	A.6	A.7	见I/O单元和接口
E/E/PE安全相关系统之间的信息交换	A.7	A.8	见数据路径/总线
分隔开电力线和信息线	A.11.1	高	应使用本表中的技术，也推荐使用其他技术
多线路的空间分隔	A.11.2	高	
提高抗干扰性	A.11.3	高	
抗合成信号传输	A.11.4	高	
注1：本表不取代附录C的任何要求。 注2：附录C的要求与诊断覆盖率的确定有关。 注3：有关本表的一般注释，见表A.1前的正文。			

表A.14 传感器

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
无功电流原理	A.1.5	低	仅对无需连续控制未达到或保持EUC安全状态的E/E/PE安全相关系统才有效
模拟信号监视	A.2.7	低	
测试模式	A.6.1	高	
输入比较/表决（1oo2，2oo3或更好的冗余）	A.6.5	高	仅当诊断测试间隔内数据流改变时才有效
参考传感器	A.12.1	高	依赖于失效检测的诊断覆盖率
可靠启动的开关	A.12.2	高	

注1 ：本表不取代附录C的任何要求。
注2：附录C的要求与诊断覆盖率的确定有关。
注3：有关本表的一般注释，见表A.1前的正文。

表A.15 最终元件(执行器)

诊断技术/措施	见IEC61508.7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A.1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
继电器触点监视	A.1.2	高	
无功电流原理	A.1.5	低	仅对无需连续控制来达到或保持EUC安全状态的E/E/PE安全相关系统有效
测试模式	A.6.1	高	
监视	A.13.1	高	依赖于失效检测的诊断覆盖率
多个执行器的交叉监视	A.13.2	高	

注1：本表不取代附录C的任何要求。
注2：附录C的要求与诊断覆盖率的确定有关。
注3：有关本表的一般注释，见表A.1前的正文。

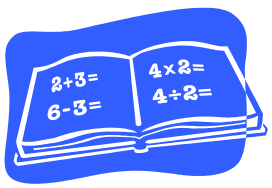
结构约束——复杂子系统

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1：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。

IS013849的指定结构



指定结构

ISO13849中的指定结构给出了每一类别的系统结构的逻辑表示。指定结构是针对SRP/CS组合而画的，它起始于触发有关安全信号，终止于动力控制元件的输出。

指定结构分为B类、1类、2类、3类和4类。其中：
B类可实现的PL最大值为PL=b，对应为SIL1；
1类可实现的PL最大值为PL=c，对应为SIL1 ；
2类可实现的PL最大值为PL=d，对应为SIL2。

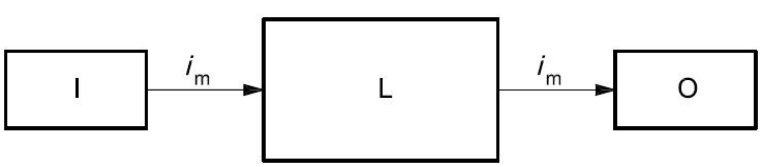
B类的指定结构

根据相关标准，运用具体应用的基本安全原则，对SRP/CS的设计、构造、选择、装配和组合至少应与有关标准保持一致并在具体应用中适应基本安全原则：

——预期的工作压力，例如：制动能力和频率的可靠性；

——工艺物料的影响，例如：洗衣机的洗涤剂；

——其他相关的外部影响，例如：机械振动、电磁影响、动力源波动或干扰。



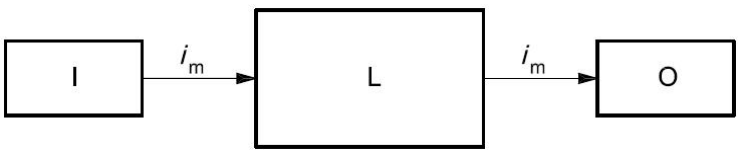
说明：
i_m 连接方式
I 输入装置，例如：传感器
L 逻辑模块
O 输出装置，例如：主接触器

可实现的PL最大值为PL=b，对应为SIL1。

类别	要求摘要	系统性能	用于实现安全的原则	每个通道的MTTFd	DCavg	CCF	可实现的PL最大值
B	SRP/CS和（或）其保护装置以及它们的元件都应根据相关标准进行设计、构造、选择、装配和组合，以使其能承受预期的影响。应使用基本安全原则	故障的发生能导致安全功能的丧失	主要特征是元件的选择	低至中	无	无关	b

1类的指定结构

1类的SRP/CS应满足B类的要求，同时采用**经验证**的元件和**经验证**的安全原则来设计和构造。



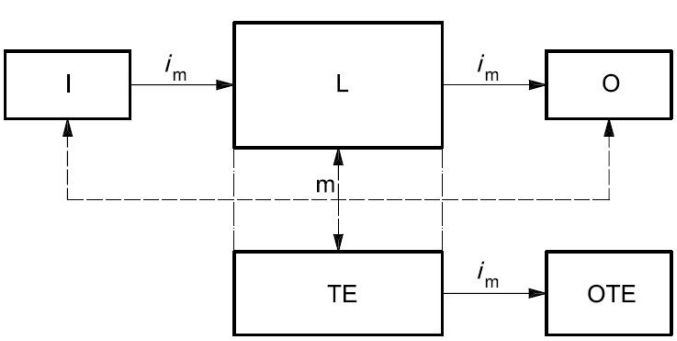
说明：
i_m 连接方式
I 输入装置，例如：传感器
L 逻辑模块
O 输出装置，例如：主接触器

可实现的PL最大值为PL=c，对应为SIL1。

类别	要求摘要	系统性能	用于实现安全的原则	每个通道的MTTFd	DCavg	CCF	可实现的PL最大值
1	应采用B类的要求。应使用经验证的元件和经验证的安全原则	故障的发生能导致安全功能的损失，但发生的概率低于B类的概率	主要特征是元件的选择	高	无	无关	c

2类的指定结构

2类SRP/CS的设计应满足B类的要求，另外还应使其功能能按照**适当的时间间隔**通过机器控制系统进行检查。



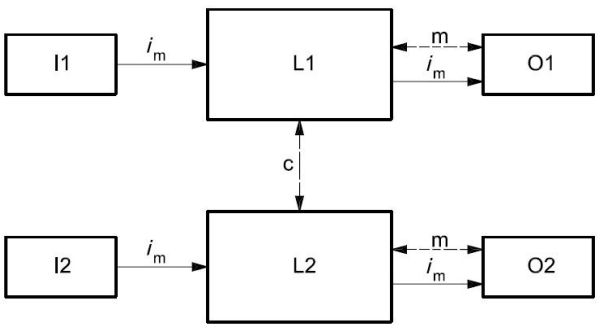
虚线代表合理可行的故障检测
说明：
i_m 连接方式
I 输入装置，例如：传感器
L 逻辑模块
m 监测
O 输出装置，例如：主接触器
TE 试验设备
OTE TE的输出

可实现的PL最大值为PL=d，对应为SIL2。

类别	要求摘要	系统性能	用于实现安全的原则	每个通道的MTTFd	DCavg	CCF	可实现的PL最大值
2	应采用B类的要求和经验证的安全原则 应通过机器控制系统以适当的时间间隔检查安全功能	在两次检查之间发生故障能导致安全功能的丧失 通过检查来检测安全功能的丧失	主要以结构为特征	低至高	低至中	见附录F	d

3类的指定结构

3类的SRP/CS的设计应满足B类的要求，另外还应使得任何这些部件中的单一故障都不会导致安全功能丧失。只要合理可行，在有关安全功能的下一指令发出时或发出之前应检测出单一故障。



虚线代表合理可行的故障检测

说明：

i_m 连接方式

c 交叉监测

I1、I2 输入装置，例如：传感器

L1、L2 逻辑模块

m 监测

O1、O2 输出装置，例如：主接触器

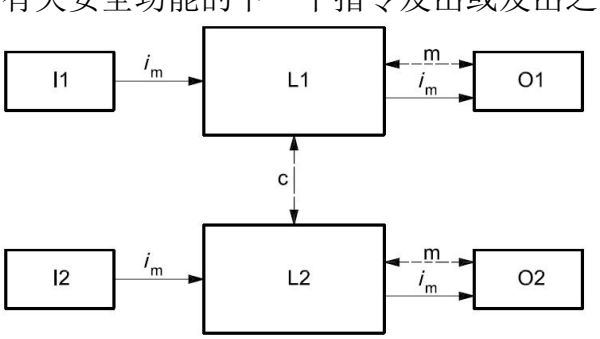
类别	要求摘要	系统性能	用于实现安全的原则	每个通道的MTTFd	DCavg	CCF
3	应采用B类的要求和经验证的安全原则；有关安全部件的设计应使： ——在这些部件中的任何一个部件的单一故障都不会导致安全功能的损失，以及 ——只要合理可行，都可检测到单一故障	当发生单一故障时，安全功能总是有效； 某些但不是全部故障将被检测到； 未检测到故障的积累能导致安全功能的丧失	主要以结构为特征	低至高	低至中	见附录F

4类的指定结构

4类SRP/CS的设计应满足B类的要求，另外还应使得：

——在这些安全相关部件中的任一部件的单一故障都不会导致安全功能的损失；

——在有关安全功能的下一个指令发出或发出之前检测到单一故障。



用于监测的实线代表诊断覆盖率，该诊断覆盖率大于3类中指定结构的诊断覆盖率。

说明：

i_m 连接方式

c 相互监测

I1、I2 输入装置，例如：传感器

L1、L2 逻辑模块

m 监测

O1、O2 输出装置，例如：主接触器

类别	要求摘要	系统性能	用于实现安全的原则	每个通道的MTTFd	DCavg	CCF
4	应采用B类的要求和经验证的安全原则；有关安全部件的设计应使： ——在这些部件中的任何一个部件的单一故障都不会导致安全功能的损失，以及 ——在下一个有关安全功能指令发出时或发出前检测到单一故障。如果不可能，则未检测到的故障的积累不应导致安全功能的损失	发生单一故障时，安全功能总是有效； 故障积累的检测减小了安全功能损失的概率（高DC） 故障将被及时检测到，以防安全功能的丧失	主要以结构为特征	高	高（包括故障积累）	见附录F

结构示例一

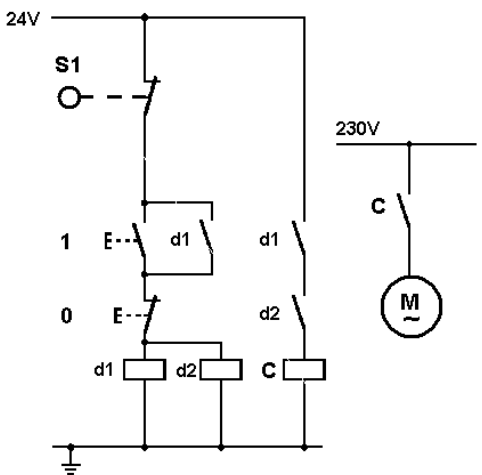
该系统设计包括：

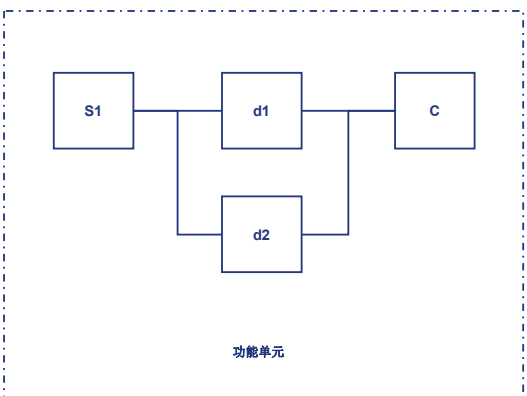
——1个安全开关 S1；

——2个关联的继电器 d1 & d2；

——1个触电器 C；

——标准按钮开关若干I/O





结构示例二

该系统设计包括：

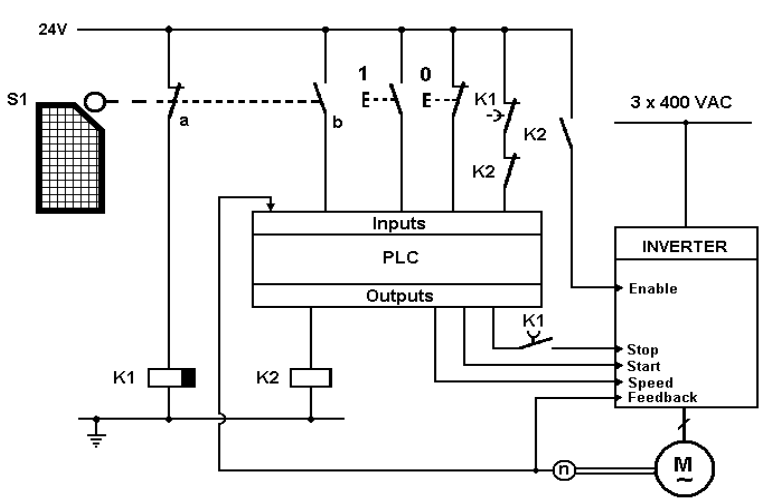
——1个具有两个触点NC/NO的安全开关S1；

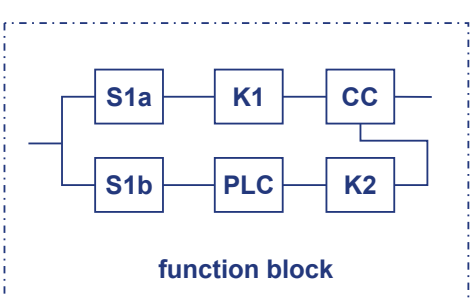
——2个关联的继电器 K1&K2；

——标准按钮开关若干 I/0；

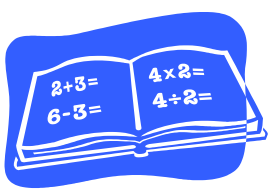
——1个标准PLC，MTTFd = 15y；

——1个变极器，MTTFd = 15 y；



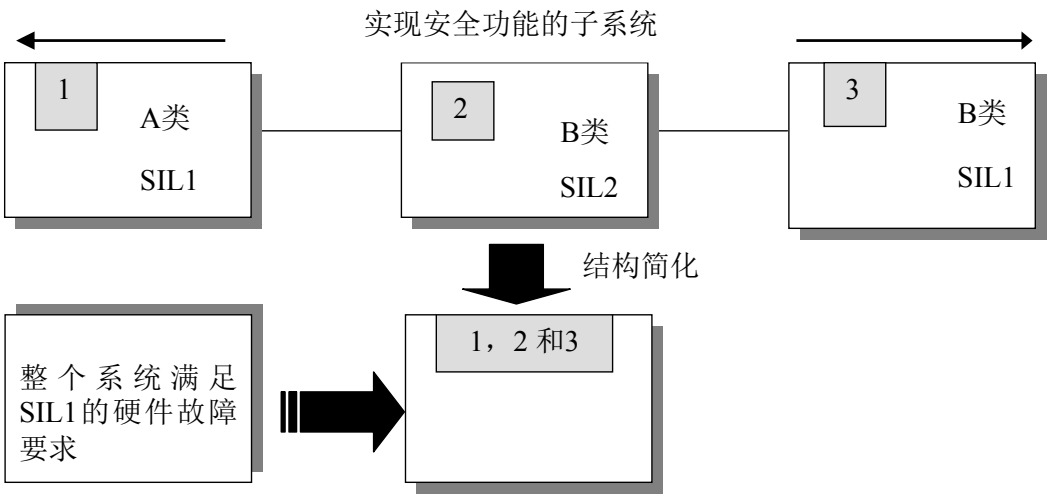


组合部件的SIL计算



单通道安全功能的硬件安全完整性限制

在E/E/PE安全相关系统中，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

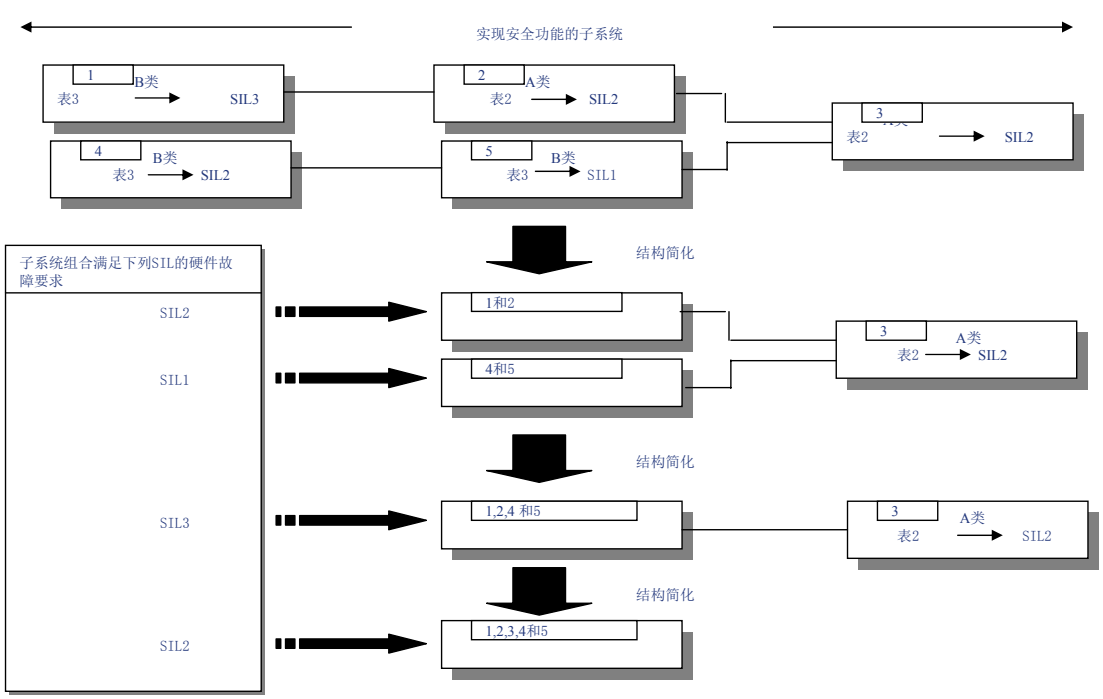
在E/E/PE安全相关系统中，若某个安全功能是通过其子系统的多个通道实现的，该安全功能所能声明的最大硬件安全完整性等级取决于：

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

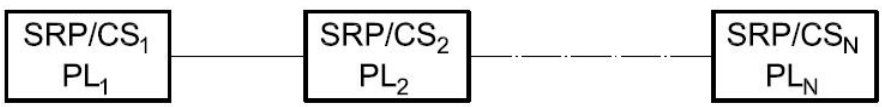
c) 分析这些组合以确定整体硬件安全完整性等级。

多通道安全功能的硬件安全完整性的限制



组合SRP/CS的PL计算

假定作为一个整体执行安全功能的串联SRP/CS分为N个单独SRP/CS_i。对于每个SRP/CS_i，其PL_i已经算出。此情形由下图所示。



执行安全功能的整个SRP/CS组合的PL的计算方法：

a）确定最低的PL_i：PL_{low}；

b）确定SRP/CS_i的个数N_{low}，$N_{low} \leqslant N$且 $PL_i = PL_{low}$；

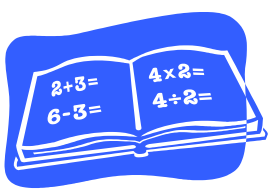
c）查询表11中的PL。

组合SRP/CS的PL计算

表11 串联SRP/CS的PL的计算

PL_{low}	N_{low}	⇒	PL
a	> 3	⇒	无，不允许
	⩽ 3	⇒	a
b	> 2	⇒	a
	⩽ 2	⇒	b
c	> 2	⇒	b
	⩽ 2	⇒	c
d	> 3	⇒	c
	⩽ 3	⇒	d
e	> 3	⇒	d
	⩽ 3	⇒	e
注：本查询表中用于计算的值基于每个PL中点的可靠性值。			

随机硬件失效



随机硬件失效

安全完整性等级（SIL）	每小时危险失效频率(PFH)	要求时的均失效概率(PFD)	风险降低因子RRF
4	≥10^{-9}～<10^{-8}	≥10^{-5}～<10^{-4}	>10000～≤100000
3	≥10^{-8}～<10^{-7}	≥10^{-4}～<10^{-3}	>1000～≤10000
2	≥10^{-7}～<10^{-6}	≥10^{-3}～<10^{-2}	>100～≤1000
1	≥10^{-6}～<10^{-5}	≥10^{-2}～<10^{-1}	>10～≤100

性能等级（PL）	每小时平均危险失效概率1/h
a	≥ 10^{-5} ~ < 10^{-4}
b	≥ 3×10^{-6} ~ < 10^{-5}
c	≥ 10^{-6} ~ < 3×10^{-6}
d	≥ 10^{-7} ~ < 10^{-6}
e	≥ 10^{-8} ~ < 10^{-7}
注：除了每小时平均危险失效概率外，其他措施也是达到PL所必需的。	

机械工业仪器仪表综合技术经济研究所
中国功能安全中心 FSCHINA

随机硬件失效

SIL和PL的关系

PL	SIL 工作模式为高/连续
a	无对应等级
b	1
c	1
d	2
e	3

PL a级与SIL无对应的等级，它主要用于轻微的风险减小，通常与伤害可逆。SIL4专门用于流程工业中可能的灾难事件，所以SIL的范围与机器的风险无关。因此与SIL3对应的PL e级为最高的等级。

随机硬件失效—IEC61508

估算随机硬件危险失效概率时，应考虑以下因素：

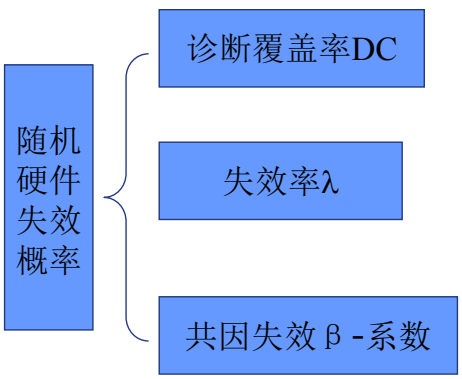
a) 与所考虑的每个安全功能相关的E/E/PE安全相关系统的结构；
b) 在任何能造成E/E/PE安全相关系统危险失效但能通过诊断测试检测到这各危险失效的模式下，估算出的每个子系统的失效率；
c) 在任何能造成E/E/PE安全相关系统危险失效但不能通过诊断测试检测到这种危险失效的模式下，估算出的每个子系统的失效率；
d) E/E/PE安全相关系统对共同原因失效的敏感性；
e) 诊断测试的诊断覆盖率和相关的诊断测试间隔；
f) 用来揭露未被诊断测试检测到的危险故障而执行检验测试的间隔；
g) 对已检测到的失效的修理时间；
h) 任何数据通信过程中未检测到的失效的概率。

随机硬件失效—IEC61508

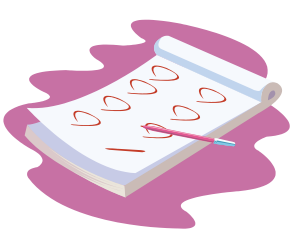
随机硬件失效概率的计算

1. PFD/PFH的计算
2. 诊断覆盖率 DC的确定
3. 失效率的确定
4. 共因失效因子的确定

…



PFD/PFH的概念



PFD/PFH

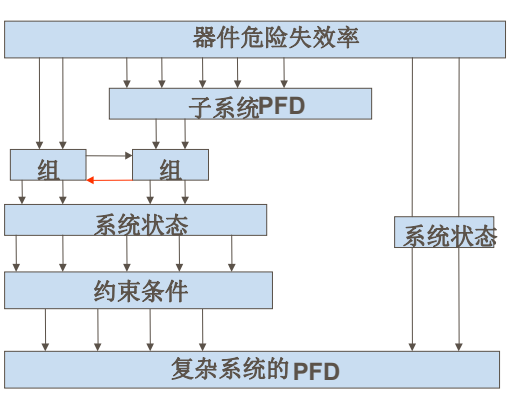
定义：

PFD-要求时的平均失效概率（Probability of Failure on Demand），对应低要求操作模式

PFH-每小时的失效率（Probability of Failure on Demand），对应连续操作模式

PFD/PFH

系统PFD：用可靠性模型，可以定量地计算出系统PFD值。

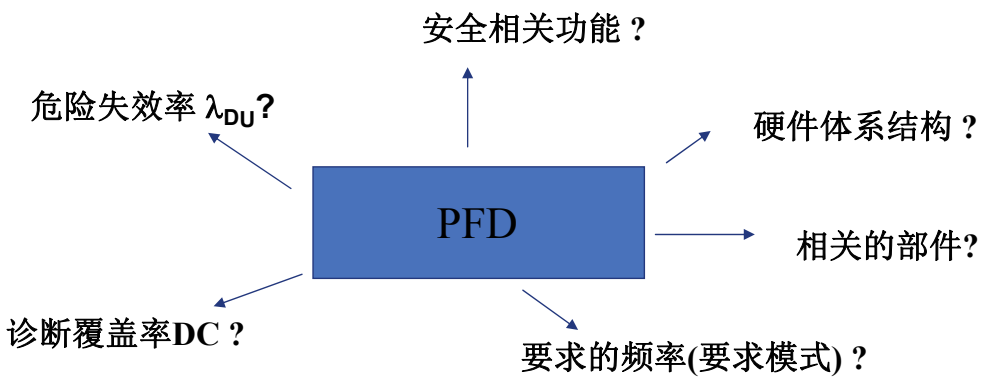


系统SIL计算过程

系统PFD取决于：

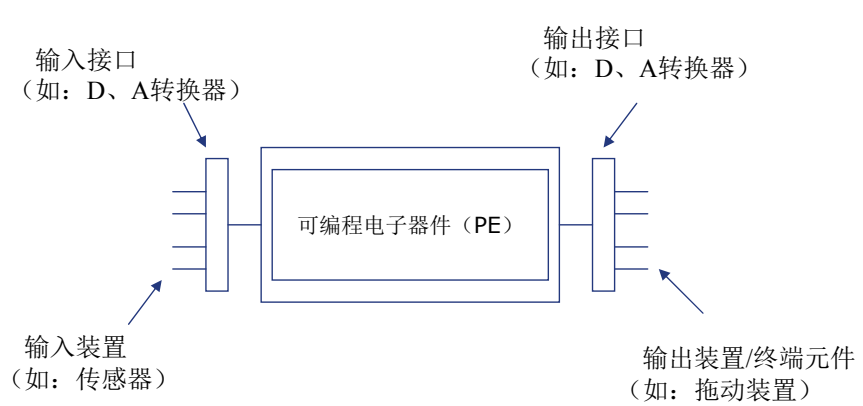
- **◆每个器件的失效率；**
- **◆系统结构；**
- **◆系统状态；**
- **◆约束条件；**

PFD/PFH



PFD/PFH

可编程电子系统的PFD计算：

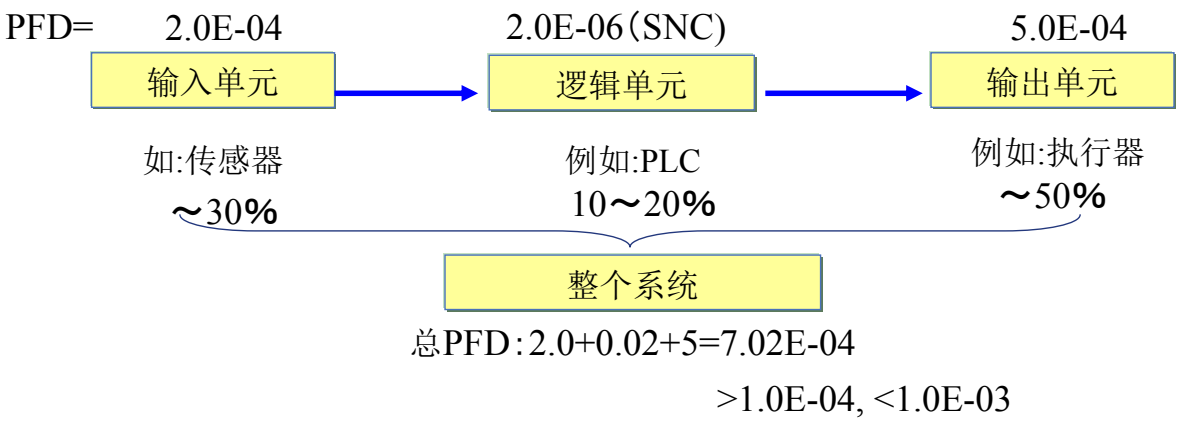


Total Loop SIL =
$PFD_{PE} + PFD_{Sensor} + PFD_{FCE}$

PFD/PFH

可编程电子系统PFD计算实例：

检验测试间隔时间 = 1年 ＝8760小时

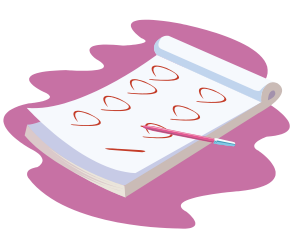


总PFD：2.0+0.02+5=7.02E-04

>1.0E-04, <1.0E-03

SIL3

共因失效因子



共因失效因子β

定义：

共同原因失效：一种失效，它是一个或多个事件导致的结果，在多通道系统中引起两个或多个分离通道同时失效，从而导致系统失效。

-- 系统性的，和

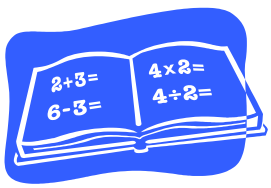
-- 随机硬件的

共因失效概率：由共同原因引起的危险硬件失效概率

β：具有共同原因的、没有被诊断测试检测到的危险失效分数

β_D：具有共同原因的、已被诊断测试检测到的危险失效分数

硬件随机失效概率 λ



硬件随机失效概率 λ

IEC61508-2010 ED2.0增加的失效划分

非部分失效

不执行安全功能那部分元件的失效。在计算安全功能失效率和SFF计算时均不必考虑。

无影响的失效

元件本身是执行安全功能的一部分，但其失效对安全功能没有直接影响。在计算安全功能失效率和SFF计算时均不必考虑。

硬件随机失效概率 λ

高位失效

当一个失效发生时会使系统的输出电流达到上限值(>20mA)或者输出电压大于(>5V或>10V),称之为高位失效。（变送器典型失效模式）

低位失效

当一个失效发生时会使系统的输出电流达到或低于下限值(<4mA)或者输出电压低于低限值时(<1V或2V),称之为低位失效。

通告失效

当一个失效不会影响“安全”但会影响电路后续检测故障的能力时（例如，诊断电路的故障），将该类失效称之为通告失效。在计算SFF时将该类失效归类为安全的、不可检测的失效。

硬件随机失效概率 λ

获得：

美军标　MIL-HDBK-217F
国军标　GJB 299b
供应商产品数据库，如西门子公司的SN29500
工业数据库，如CCPS,OREDA
用户使用中记录收集的现场数据
。。。

单个元件$MTTF_d$值的计算

$MTTF_d$定义为平均危险失效时间。

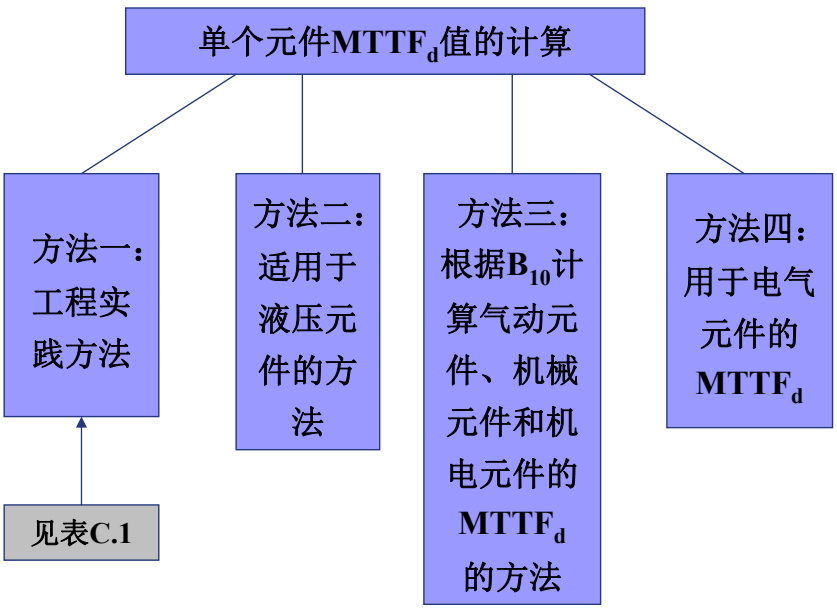
对于单个元件$MTTF_d$的计算，应按以下顺序得到$MTTF_d$的值：

a）采用制造商的数据；

b）使用附录C和附录D的方法；

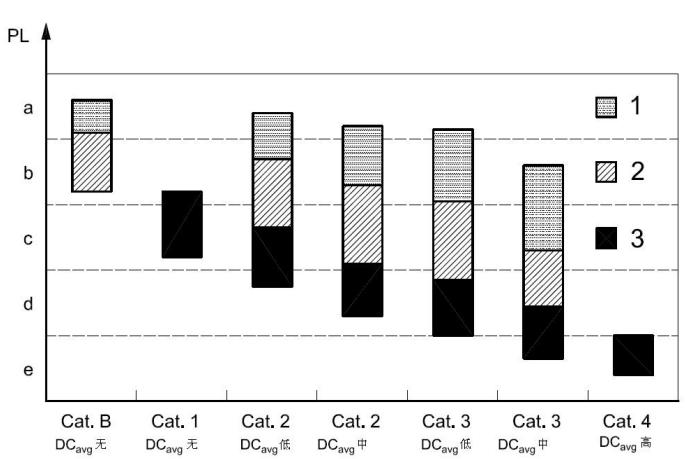
c）选为10年。

单个元件$MTTF_d$值的计算



性能等级PL的估计

PL和每个通道的类别、DC_{avg}和$MTTF_d$的关系



说明：

PL 性能水平

1 每个通道的MTTFd = 低

2 每个通道的MTTFd = 中

3 每个通道的MTTFd = 高

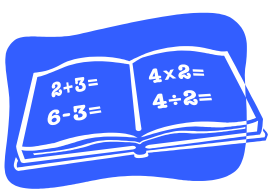
类别和DC_{avg}的组合确定选择图中的那一列。根据每个通道的$MTTF_d$，选择有关直方柱的3个不同阴影区域中的一个。这些区域的纵向位置确定能在竖轴上读出的PL。如果该区域有两种或三种可能的PL，表7给出了所达到的PL。数字更精确的PL的选择取决于每个通道MTTFd的精确值，见附录K。

性能等级PL的估计

表7 估计由SRP/CS达到的PL的简单程序

类别		B	1	2	2	3	3	4
DC_{avg}		无	无	低	中	低	中	高
每个通道的 $MTTF_d$								
	低	a	不包括	a	b	b	c	不包括
	中	b	不包括	b	c	c	d	不包括
	高	c	c	c	d	d	d	e

数据通信的要求



数据通信的要求

◆ 当在安全功能的实现中使用任何数据通信格式时，那么在估算通信过程中未检测到的失效概率时，应将传输差错、重复、删除、插入、重新排序、误用、延时和伪装等因素考虑进去在估算由随机硬件失效引起安全功能危险失效的概率时应考虑此概率。

注：伪装一词的意思是报文的真实内容没有被正确地鉴别。例如，来自非安全部件的报文错误地被鉴别为来自安全部件的报文。

◆ 特别是在估算由通信过程引起安全功能失效的概率时，应考虑如下参数：

a）残余错误率（见IEV 371-08-05）；

b）残余信息丢失率（见IEV 371-08-09）；

a）信息传送率（比特率）的限制和可变性；

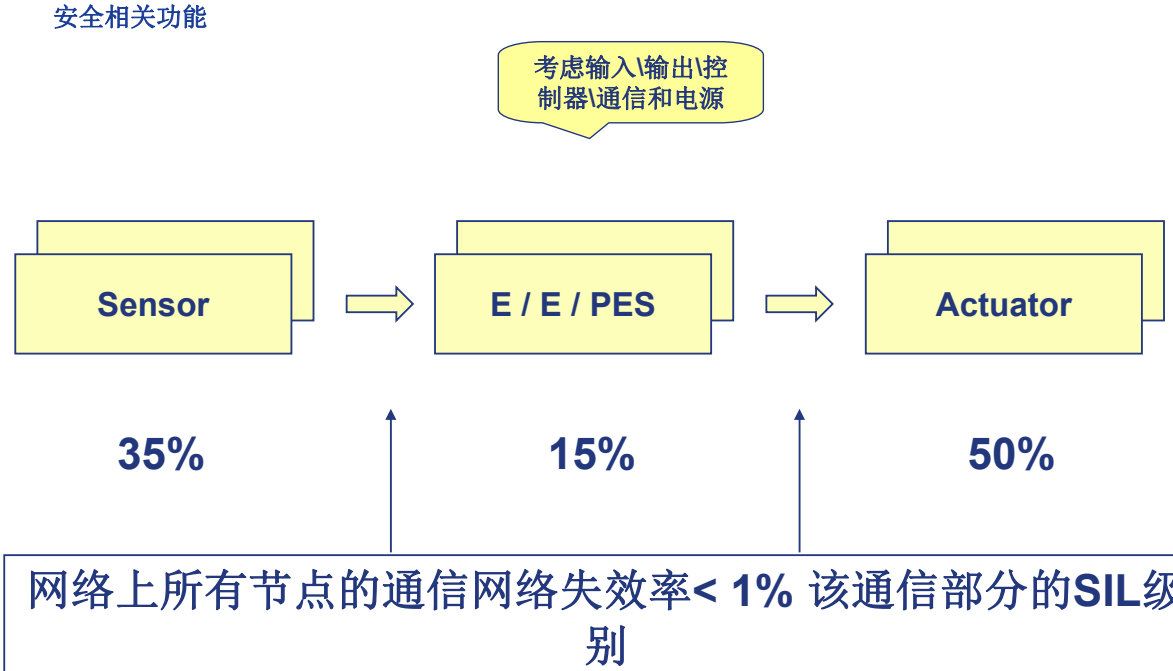
d）信息传播延时的限制和可变性。

注1：每小时危险失效率等于残余错误率除以报文长度（二进制数位）乘以与安全有关的报文的总线传输率再乘以系数3600。

注2：进一步信息可见IEC60870-5-1、EN50159-1和EN50159-2。

网络上所有节点的通信网络失效率要求

安全相关功能



谢谢！

机械工业仪器仪表综合技术经济研究所　功能安全中心主任
全国工业过程测量控制与自动化标准化技术委员会
系统及功能安全分技术委员会 副主任委员

史学玲教授
sxl@instrnet.com
13466515782，010-63461376

功能安全中心网址：www.fs-china.org