综述与评论

# 降低机车车辆电子产品及其系统风险的对策

严云升，周桂法

（株洲南车时代电气股份有限公司 技术中心，湖南 株洲　412001）

作者简介：严云升（1940-），男，高级工程师（教授级），从事电力机车微机控制系统的开发设计工作；

周桂法（1964-），男，高级工程师（教授级），株洲南车时代电气股份有限公司首席专家，从事机车、列车微机网络控制及故障诊断方面的研究开发工作。

**摘　要**：从硬件和软件可靠性设计、保护、故障诊断和冗余几方面阐述了降低机车车辆电子产品及其系统风险的各种措施及其有效性。在产品设计阶段，就必须考虑各种降低风险的对策，采取行之有效的措施，才能得到高安全完整性的产品。

**关键词**：安全完整性；风险；可靠性；故障诊断；冗余；机车车辆

**中图分类号**：U298　　**文献标识码**：A　　**文章编号**：1000-128X(2006)05-0001-04

## Countermeasures to Reduce Risks of Electronic Components and System for Rolling Stock

YAN Yun-sheng, ZHOU Gui-fa

(Technology Center, Zhuzhou CSR Times Electric Co., Ltd., Zhuzhou, Hunan 412001, China)

**Abstract:** Various measures and their effectiveness to reduce the risks of electronic components and system for rolling stock are illustrated from aspects of hardware, software reliability design, protection, failure diagnosis and redundancy. During the phase of product design, the measures to reduce the risks must be taken into account and effective measures should be taken to achieve products of high safety integrity.

**key words:** safety integrity; risk; reliability; failure diagnosis; redundancy; rolling stock

## 0　引言

机车车辆上的电气/电子/可编程电子（简称E/E/PE）安全相关系统，其安全完整性级别（简称SIL）分成４级，最高的SIL4，每小时危险失效的概率应在$10^{-9}$～$10^{-8}$之间；每降低一级，其每小时危险失效概率递增一个数量级；最低的SIL1，每小时危险失效的概率应在$10^{-5}$～$10^{-6}$之间。在现有元器件水平和工艺条件下，对于不太复杂的系统，是不难实现SIL4的；但对于一个相对复杂的系统（例如可编程电子安全相关系统），要实现SIL4就必须采取许多相关的措施。

一般可编程电子安全相关系统可由３部分组成：传感器子系统，逻辑控制子系统和最终部件子系统，这３个部分互相串联。

对于串联的子系统，如果子系统的SIL不同，则串联后最高只能达到其中最低的SIL级，假定３个子系统的SIL分别为1，3，2级，则串联后整个系统最高只能达到SIL1级。因而要找出串联系统中最薄弱的环节，对其采取一定措施方能提高整个系统的SIL等级。在采取一定措施后，原来最薄弱的环节失效率得到改善，其他环节有可能又成为最薄弱环节。如此对最薄弱环节不断采取有效措施，直至最后整个系统达到预定的SIL级别的要求。

在确定安全功能的安全完整性时，首先要分析可能导致不安全状态的所有失效原因。例如硬件失效、软件引发的失效、电气干扰引起的失效或是人为操作引起的失效等。降低风险的对策一是要避免这些隐患的发生（避错），二是在故障发生时采取措施不致使系统失效（容错）。

## 1　硬件可靠性设计

如图１所示，在明确产品的工作条件，主要输入和输出参数（设计输入）后，首先要进行安全性设计，目标是开发总体安全要求规范，包括安全功能要求和安全完整性要求。为此要对产品进行隐患和风险分析，得到该产品可能具有的风险；对每个已确定的隐患规

收稿日期：2005-12-17；收修改稿日期：2006-06-29

定所必需的安全功能，以保证所需的功能安全性。同时根据该产品的作用和重要性，确定各安全功能的危害严酷等级，确定所需的安全完整性级别，亦即得到该产品容许的风险。

为了把产品的风险降到容许风险以下，使其成为可接受的产品，必须进行可靠性设计。总体而言，系统的可靠性依赖于组成系统的各个零部件的可靠性。所以，提高零部件的可靠性是提高系统可靠性的根本途径。如果将零部件的失效率降低 1 个数量级，系统的安全完整性就可以提高一个等级。系统的可靠性还与系统的复杂程度相关。简化系统的复杂性，可以提高系统工作的可靠性。所以在系统设计时，在不影响系统基本性能的前提下，应尽量简化系统结构。

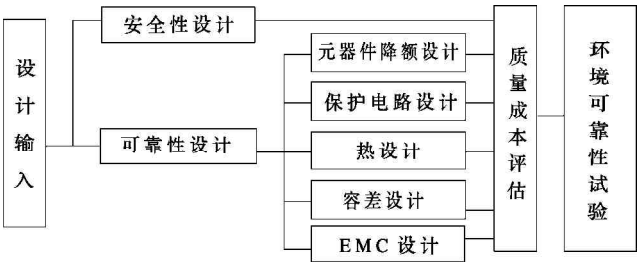



图 1 产品可靠性设计流程图

常用的可靠性设计措施有：

①元件降额设计。目的是降低发热和应力，从而减少故障率，这是一种“避错”措施。通常，在降低使用应力水准的情况下，其可靠性可以提高一个数量级以上[1]。

②热设计。热设计也是一种“避错”措施。热设计对电子产品是非常重要的，通常电子产品的热容量比较小，对温度比较敏感。除了选择适当级别的元器件外，还可以考虑以下措施：一是借助车体通风来降低电子产品周围的环境温度；二是电子柜自身的通风和热交换，把热量散发出去。在通风的同时还需保持电子产品的清洁。因而往往采用内外 2 层风道。内风道是封闭的，它通过空气流动使温度均匀并保持产品清洁；外风道靠通风将散热器上的热量带走。对于没有强迫通风的产品也需考虑发热体与周围器件的距离以及安装方式，以减少对邻近元器件的影响。对于需在特殊低温环境下工作的情况，还需考虑低温下的启动问题。

③容差设计。这是一种“容错”措施。元器件的输入有一定容许范围，对可能的过大信号应采取钳位限制措施。例如计算机的 A/D 转换都有一定范围，对于输入的模拟信号最好采用钳位限制，以免烧损 A/D 芯片。

④保护。保护是一种“容错”措施。保护措施的作用详见本文的第 3 部分。

⑤EMC 设计。产品的 EMC 设计是可靠性设计中的重要部分。机车车辆上空间受到限制，各种强电设备（如牵引变压器、牵引变流器）和弱电设备（如各种电子控制装置）往往紧凑地布置在一起。电子产品要能满意地工作，自身必须有一定的承受外界电磁干扰的能力，同时它对外界的干扰也必须限制在一定水平以内。机车车辆上的电子产品的 EMC 一般应满足恶劣的工业环境要求。TB/T3021-2001《铁道机车车辆电子装置》标准中规定了电子产品必须进行的 EMC 试验项目和考核等级；产品须通过 EMC 试验才能上车。实践证明这对于提高产品质量和可靠性确实起到了重要的作用。

提高产品的抗电磁干扰能力一般都从屏蔽、滤波、隔离和接地 4 个方面下功夫。只要这几种措施得当，一般可以达到规定的 EMC 要求，当然需要有不断改进、不断试验的过程，才能得到较为完美的产品。除了产品自身的 EMC 设计外，还需考虑它在机车上的安装条件和布线要求，如安装在具有磁屏蔽功能的小室内，接地线的截面和接地点的选择，采用什么样的导线和电缆以及这些电缆与动力线间的距离等。

当产品在实际工作中受到干扰而有时不能正常工作时，还须从系统的角度分析干扰的来源和采取必要的措施。如 $SS_{7D}$ 机车一开始头灯每次起辉时总引起显示屏的闪动，原因是头灯起辉时有较高的过电压，他影响到 110 V 蓄电池电路，引起显示屏闪动，后将头灯的电源线改用双绞屏蔽线后，这一问题得以解决。

## 2 软件可靠性设计

一个软件系统的可靠性很大程度是在系统设计阶段就已经决定了的，换句话说，如果在软件系统的设计时没有对软件可靠性问题给予很好的考虑，以致设计水准较低的话（如系统结构不佳、可读性不好），则即使在系统调试过程中投入很大资源，也很难得到一个高可靠性的软件系统。因此在软件设计阶段，设计者就应对产品设计可能影响其可靠性的因素，如结构、编写方法等给以足够的重视。

软件设计之初首先要编制软件要求规范。根据系统要求规范，系统安全性要求规范和系统结构描述来确定分配至软件的全部安全功能。应明确软件与任何其他系统间的接口，包括与操作员的接口，对于可能出现的人为操作错误应采取安全导向措施；明确软件与硬件间的任何约束，确定软件自检的程度及由软件检测硬件的程度；明确软件的安全完整性等级并确定诊断测试的范围和周期。

目前，从理论上讲还没有真正解决怎样得到一个高可靠的软件产品问题，而只是利用某些方法、技巧和经验来提高软件的可靠性：

①限制跳转语句的使用。任何一种程序逻辑结构都可以用顺序、选择和循环 3 种基本结构组成的单一进出口逻辑结构来实现。

②从上到下程序设计法（简称下行法）。下行法基本上是一个分解的过程，他侧重于程序的控制结构。首先是整个软件系统的最抽象最综合的描述，然后将软件分解成若干个独立的模块并分别进行设计描述。如果需要的话，再将一个模块分解成若干子模块，这种分解重复进行直到每个最后的子模块可以用比较简单、直观的方法编写为止。这种方法的一个特点是：在进行较低一级的描述与设计时，其上一级已经有了完整的描述与设计。在模块之间只有必要的数据和信息传递，而没有过多的耦合。这样做使软件控制结构清晰，有较好的可读性、可维修性和可靠性。

③模块式结构。每个模块相对独立，功能单一并且模块只有一个进出口。从而防止错误在模块之间的扩散传播，可以提高软件的可靠性。

④软件须通过测试验证。软件测试分成3个阶段：模块测试、软件集成测试和软/硬件集成测试。

在一定置信度下，为验证软件失效率符合某个SIL级别所需验证的次数和时间见表1。

**表1　软件置信度所需的次数和时间[3]**

| SIL | 低需要工作模式按需要执行设计功能的失效概率 | 处理需要的次数 | | 高需要或连续工作模式每小时危险失效的概率 | 总的工作时间/h | |
|---|---|---|---|---|---|---|
| | | 1- $\alpha$ =0.99 | 1- $\alpha$ =0.95 | | 1- $\alpha$ =0.99 | 1- $\alpha$ =0.95 |
| 4 | $\geq 10^{-5}\sim<10^{-4}$ | $4.6\times10^{5}$ | $3\times10^{5}$ | $\geq 10^{-9}\sim<10^{-8}$ | $4.6\times10^{9}$ | $3\times10^{9}$ |
| 3 | $\geq 10^{-4}\sim<10^{-3}$ | $4.6\times10^{4}$ | $3\times10^{4}$ | $\geq 10^{-8}\sim<10^{-7}$ | $4.6\times10^{8}$ | $3\times10^{8}$ |
| 2 | $\geq 10^{-3}\sim<10^{-2}$ | $4.6\times10^{3}$ | $3\times10^{3}$ | $\geq 10^{-7}\sim<10^{-6}$ | $4.6\times10^{7}$ | $3\times10^{7}$ |
| 1 | $\geq 10^{-2}\sim<10^{-1}$ | $4.6\times10^{2}$ | $3\times10^{2}$ | $\geq 10^{-6}\sim<10^{-5}$ | $4.6\times10^{6}$ | $3\times10^{6}$ |

注：表中 1- $\alpha$ 表示置信度

以高需要或连续工作模式为例，失效率 $\lambda$ 与所需测试时间 $t$ 的关系为 $t=\frac{1\mathrm{n}\alpha}{l}$。式中 $t$ 是相同软件版本在不同设备上运行时间的总和。一个软件随着运行时间的增加，其可靠性也可增长。这可根据表1来判断。

## 3　保护

一个安全相关系统即使已满足SIL4的要求，也不能说明是绝对可靠的，尽管失效率很低，但仍需要有失效时的安全对策。

失效时的安全对策一是根据“故障导向安全”的原则来设计，二是去触发保护设备动作，从而保证系统安全。该保护设备可以是该安全相关系统自带专用的，也可能是外部公用的。在安全相关系统中每加入一层保护，就对安全完整性实现了一阶量级的改善，即可提高一个安全完整性等级。通常一个E/E/PE安全相关系统往往只有一层保护，需要借助其他设备来实现2层或多层保护。例如：

制动系统事关列车安全。为提高安全性，在“中华之星”上采用3套制动系统的方案：即以微机控制的直通电空制动为主、基础制动为辅、备用空气制动用作电空制动失效时的后备保护。即除正常的制动系统外又加了2层保护，从而使制动系统的安全完整性提高了2个等级。

相控机车上的主电路采用晶闸管可控整流。封锁晶闸管触发脉冲可以解决调节不当引起的不安全因素，但对于外部引起的短路和接地，则必须切断其主电路才能消除。因而当出现过压、过流等不安全因素时，封锁触发脉冲成为首选的保护措施，与此同时，还须发出切断其主电路的命令。

对于重要的保护可以由2个以上的设备进行判断，如一次测电流信号可送到微机去判断有否过流；还可以通过一次测过流继电器来判断是否过载，只要有一个设备判断为一次测过流，都可用主断路器切断主电路，从而提高了过流保护的可靠性。

## 4　故障诊断

故障诊断的作用是在某个设备故障失效时，及时采取必要的措施，并把此信息通知司机，以防事故的发生和缩小故障范围。

电子产品故障分2类：一类是不影响安全的故障（故障率为 $\Sigma\lambda_S$）；另一类为有危险的故障（故障率为 $\Sigma\lambda_D$）。诊断系统主要是针对有危险性故障的，设在有危险的故障 $\Sigma\lambda_D$ 中，诊断系统能诊断出 $\Sigma\lambda_{DD}$，则该系统的安全故障率为 $(\Sigma\lambda_S+\Sigma\lambda_{DD})/(\Sigma\lambda_S+\Sigma\lambda_D)$，诊断覆盖率为 $\Sigma\lambda_{DD}/\Sigma\lambda_D$。

硬件故障容许 $N$ 意味着 $N+1$ 个故障可引起安全功能的丢失，$N$ 的值一般为0～2。硬件故障容许是在不考虑采取其他控制故障影响的措施（如诊断）下得到的。硬件故障容许为0意味着一旦硬件故障就有可能丢失安全功能，是高标准要求。硬件故障容许为2是低标准要求。

一个安全功能可以声称的最高安全完整性受硬件故障容许及执行该功能的子系统的安全故障率的限制。IEC61508-2电气/电子/可编程电子安全相关系统的功能安全 第2部分 对系统的安全故障率有明确规定，见表2和表3。

A型系统为成熟的系统。构成系统的所有元件的故障模式已定义，故障时子系统的行为已完全定义，对于能检测或不能检测的危险故障已有足够的经验数据。

表2 A型安全相关子系统的硬件安全完整性

| 安全故障率 | 硬件故障容许 | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| ＜60% | SIL1 | SIL2 | SIL3 |
| 60% ～＜90% | SIL2 | SIL3 | SIL4 |
| 90% ～＜99% | SIL3 | SIL4 | SIL4 |
| ≥99% | SIL3 | SIL4 | SIL4 |

表3 B型安全相关子系统的硬件安全完整性

| 安全故障率 | 硬件故障容许 | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| ＜60% | 不允许 | SIL1 | SIL2 |
| 60% ～＜90% | SIL1 | SIL2 | SIL3 |
| 90% ～＜99% | SIL2 | SIL3 | SIL4 |
| ≥99% | SIL3 | SIL4 | SIL4 |

B型系统为尚不太成熟的系统。至少有一个构成系统的元件的故障模式未定义，故障时子系统的行为不能完全定义，对于能检测或不能检测的危险故障缺少充分的经验数据。

对于硬件故障容许为1的B型SIL3系统其安全故障率必须达到90%～99%，而对危险性故障的诊断覆盖率应达到90%，根据这些数据可确定所需诊断的范围。IEC61508-2附录A对各种组件的诊断内容有初步的推荐[2]。

目前我国在机车车辆上故障诊断还处于较低的水平，诊断的广度和深度都有待于提高，在故障定位和故障原因分析上还须进一步研究。在计算机方面一般可以做到上电时对CPU、存储器以及其他控制的外设（如数字I/O、模拟I/O）进行诊断；采用比较法周期性地对各种电流、电压和速度传感器进行诊断；若出现不安全因素，则将故障前后一段时间内的数据进行记录，以便事后进行故障原因分析；对于轴承温度可以进行超温报警和记录数据；在走行部，可以诊断轴承故障及齿轮、踏面的损伤。

高速列车的主要运行功能如司机室信号、牵引传动的控制、制动、转向架的稳定性等都必须连续自动监测，并且监测功能本身在一定时间间隔内也定期地被自动测试。一旦出现异常必须采取果断的措施。对于所有可能危及运行的故障，诊断覆盖率必须大于90%。

诊断系统应根据部件的重要程度和故障危害等级形成整列车的故障评估逻辑，在几种故障同时发生时，确定整列车故障等级的升级。

在诊断处理上可以分成3个层次：

①快速反应层次。与故障相关的部件应能迅速采取故障隔离措施，以防事故扩大。

②综合反应层次。通过列车通信网络，各部件把故障信息与环境参数报告给列车主控单元，并在显示屏上显示，由司机决定下一步如何操纵列车。

③面向管理层次。将故障发生前后一段时间内的数据及环境参数记录下来供维护分析及管理用。

## 5 冗余

冗余是一种容错措施。冗余的作用是提供功能备用，不论是通道冗余，还是设备冗余，在一个通道或一个设备故障时，另一通道或另一设备仍能正常工作，从而不致使系统失效。

冗余要能真正起到作用，冗余的通道或设备必须互相独立，尽量避免因共同原因使其一齐失效。例如，将一个信号送至2个不相关的设备中，可以起到冗余作用；若将一个信号送到同一设备的不同通道中，就起不到冗余作用，一旦该设备电源故障，这个信号仍然没有通道，系统仍会失效。2个冗余的设备电源应互相独立，虽然供电电源在机车上DC 110 V只有一个，但去设备的电源线必须分别进线，而不应公共进线后2个设备并联，否则会由于电源进线断线或连线松脱，造成2个设备都不能工作。

冗余措施是很有效的，它使安全完整性提高了一个等级，例如由若干部件组成的并联系统，其可靠度$R(t)$：

$$R(t)=1-\left(1-\mathrm{e}^{-\lambda_i t}\right)^{m_i}$$

式中：$\lambda_i$——单个部件的失效率；$m$——并联的部件数。

相同部件采用并联后的故障改进系统$G$

$$G=\frac{\text{单个部件的故障概率}}{\text{并联复式部件的故障概率}}=\left[\frac{1}{1-\mathrm{e}^{-\lambda t}}\right]^{m-1}$$

根据安全完整性定义各级的平均失效率为

SIL1 $\lambda_1=5\times10^{-6}$

SIL2 $\lambda_2=5\times10^{-7}$

SIL3 $\lambda_3=5\times10^{-8}$

SIL4 $\lambda_4=5\times10^{-9}$

要求的工作时间$t$假设为20 000 h，即平均无故障时间为4年（每年工作按5 000 h计算），则：

SIL1与SIL1并联→SIL2 $G_1$=10.5

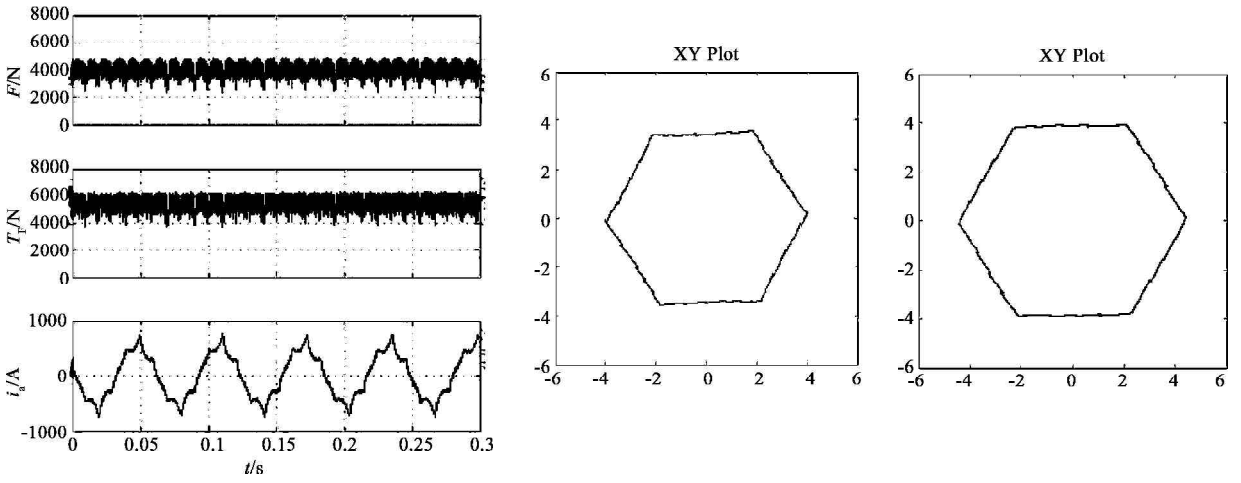
SIL2与SIL1并联→SIL3

SIL3与SIL1并联→SIL4

SIL2与SIL2并联→SIL4 $G_2$=100

由此可见：①任何SIL级与SIL1并联后，其SIL可提高一级；②由2个SIL2并联可得到最高的SIL4级。这为设计一个高安全完整性的系统提供了一种思路，即采用2个SIL2热备工作。

机车车辆上的电子装置也有不少是采用冗余的。如LCU冷备具有较高的可靠性；LKJ-2000运行监控记录装置在模块级实现了冗余；“中华之星”交流传动机车上，重要的信号都送到2个设备中，从而提高了可靠性。交直传动电力机车上，通常把司 （下转第19页）




（a） 电流及推力比较图　　（b）磁链比较图

图 7　互感下调 15%的直接推力控制仿真结果图

有算法简单有效、推力响应快的直接推力控制系统，对于直线电机的控制是一种有效可行的控制策略。这种控制策略对参数的依赖程度低，而基于该电机模型的直接推力控制对高速时被削弱了的气隙磁场也进行了有效补偿。其鲁棒性在仿真中也初步得到验证。但影响直线电机参数的原因多，参数变化较大，与旋转电机控制系统比较，性能稍差。为提高控制系统鲁棒性和控制性能，值得进一步的分析和研究。

**参考文献：**


[1] 浙江大学电机教研室. 直线感应电动机 [M]. 北京：科学出版社，1978.

[2] 上海工业大学，上海电机厂. 直线异步电动机[M]. 北京：机械工业出版社，1979.

[3] 叶云岳. 直线电机原理与应用 [M]. 北京：机械工业出版社，2000.

[4] Jawad Faiz, H Jafari. Accurate Modeling of Single-sided Linear Induction Motor Considers End Effect and Equivalent Thickness [J]. IEEE Trans.on Mag., 2000(5), 3785-3790.

[5] Roberto H Manno, Eduardo Galvan Diez. Direct Force Control for a three-phase double-sided Linear Induction Machine with transverse magnetic flux [J]. Conference record of the 2002 IEEE, 2002(04), 2826-2831.

[6] J Duncan. Linear Induction Motor—Equivalent Circuit Model [J]. IEE Proc., 1983(1):51-57.

[7] 李　夙. 异步电动机直接转矩控制 [M]. 北京: 机械出版社，1999.

[8] Bahram Amin. Induction Motors [M]. Berlin：Springer,2002.

[9] R M Pai, Ion Boldea. A Complete Equivalent Circuit of A Linear Induction Motor With Sheet Secondary [J]. IEEE Trans. on Mag., 1988(1):639-654.

[10] T A Lipo, T A Nondahl. Pole-by-pole d-q model of a linear induction machine [J]. IEEE Trans. on power apparatus and system, 1979(2):629-642.


（上接第4页）　机重要指令同时送到2个转向架的控制箱中，而这2个控制箱采用独立电源进线。模拟控制的交直传动机车采用A、B组控制，在A组故障时改用B组控制，从而保证了机车的主要功能。而微机控制的交直机车上，正常位时为2个转向架独立控制，故障位改为由完好的一个转向架进行集中控制，有故障的转向架则跟随触发，从而在硬件增加不多的情况下仍然实现了基本的牵引和电制动功能。

## 6　结束语

①改善零部件的可靠性和简化系统是提高系统可靠性的根本途径，采取降额设计、热设计、容差设计和EMC设计，要在前面二者之间寻求平衡，以得到最高的可靠性。

②软件采用结构式程序设计有较好的可读性、可靠性和维护性。

③每加入一层保护，可在安全完整性上提高一个等级。

④对于SIL3的B型系统，其安全故障率必须达到90%～99%，而对危险性的故障诊断覆盖率应达到90%。

⑤任何SIL级与SIL1并联后，其SIL可提高一个等级；由2个SIL2并联，可得到最高的SIL4。这为设计高安全完整性的系统提供了一种思路。

**参考文献:**


[1] 陈开运. 牵引电气设备及系统的可靠性设计初探 [J]. 机车电传动，2004(3)：63－65.

[2] IEC61508-2，电气/电子/可编程电子安全相关系统的功能安全性 第2部分 电气电子可编程电子安全相关系统的要求 [S].

[3] 周桂法，严云升. 铁路产品的风险和安全完整性 [J]. 机车电传动，2006(4):1-4