综述与评论

机车电子产品的RAMS

严云升
(株洲电力机车研究所 研发中心,湖南 株洲 412001)

作者简介:严云升(1940-),男,1962年毕业于上海交通大学电力机车专业,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。

摘 要:根据IEC 62278-2002提出的铁道风险评估框架,阐述了铁道机车车辆电子产品的RAMS,对电子产品危害出现的频度进行了量化,对各种电子产品可能引发的危害严重等级进行了细化,并提出降低风险的3种设计对策。

关键词:机车车辆;电子产品;可靠性;可用性;可维护性;安全性;风险;冗余设计
中图分类号:U26 **文献标识码**:A **文章编号**:1000-128X(2003)06-0001-04

RAMS of electronic products for railway rolling stock

YAN Yun-sheng

(R & D Center, Zhuzhou Electric Locomotive Research Institute, Zhuzhou, Hunan 412001, China)

Abstract: On the basis of railway risk evaluation framework proposed by IEC62278-2002, the RAMS of electronic products for rolling stocks are presented. The frequency of the hazards caused by electronic products is quantitated. Possible hazards are classified and 3 design countermeasures are put forward to reduce the hazards.

Key words: rolling stock; electronic product; reliability; availability; maintainability; security; risk; redundancy design

1 RAMS简介

RAMS是可靠性(Reliability)、可用性(Availability)、可维护性(Maintainability)和安全性(Safety)英文第一个字母的组合。RAMS是系统长期工作的特性,它是在系统的寿命周期内,通过对工程概念、方法、工具和技术的应用获得的。系统的RAMS可用质量和数值来表示系统、子系统或组成系统的部件的性能程度,它是系统可靠性、可用性、可维护性及安全性的组合,这四者之间的关系如图1所示。

可靠性:某个项目在给定条件和给定时间间隔内,能执行所要求功能的几率。

可用性:在规定的一段时间或一定的时间间隔内,假定所有的外部资源均满足,产品处于能完成所要求功能的状态之时间的比率。

维修性:在给定情况下使用的某个产品于规定时间内,在规定条件下用规定的程序和资源有效地完成维护作业的概率。

收稿日期:2003-06-30

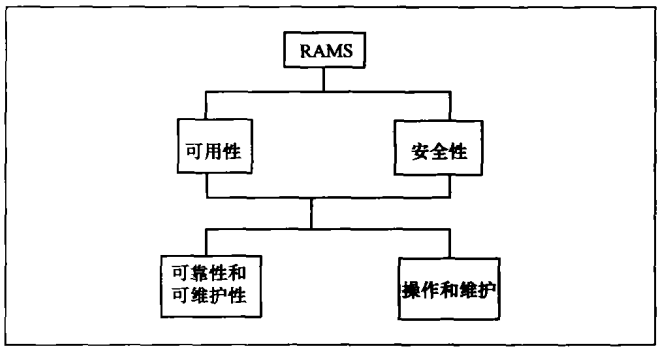

图1 RAMS各组成部分间的相互关系

安全性:没有非允许损坏的危险。

安全完整性:在给定时间和所有规定条件下,系统满意地实现所要求功能的可能性。

关于铁道RAMS国际上先有EN50126: 1999标准,现在该标准已上升为IEC 62278: 2002 铁路应用——铁道可靠性、可用性、可维护性和安全性(RAMS)规范及说明。学习和贯彻该标准有利于了解我们产品现在的水平、提高产品的质量,与国际接轨。

在国内及香港的招标文件中,对系统或产品都有可靠性、可用性、可维护性及安全性要求的相关章节。

在标书中可靠性用平均无故障时间MTBF(计算值)表示；可用性用实际可用的时间对全运行时间的比率表示；可维护性用识别判断故障及恢复到正常状态平均所需的时间以及维护方便性来表示，以便能在运行安排的间隙中完成维修；安全性需通过风险评估，达到可接受的风险等级。

2 铁道产品的风险评估

铁道产品的风险用出现危害事件的频度及危害的严重等级的矩阵来评估。

在IEC 62278中，对于危害事件出现的频度分成6个等级，对危害的严重等级分成4级，对质量风险分成4级，分别见表1、表2、表3。该标准中给出了风险评估矩阵的例子，见表4。

表1 出现危害事件的频度

分类	定 义
频繁	频繁地出现，危害将一直存在
经常	发生多次，危害可以预期经常发生
有时	可能发生几次，危害预期有几次发生
很少	在系统寿命周期的某个时期可能发生，危害有理由预期发生
极少	不太可能发生，危害可视为例外出现
几乎不可能	几乎不可能发生，危害可以视为不会发生

表2 危害的严重等级

严重等级	对人或环境的影响	对运行的后果
特大	致命性的，或是多方面的严重伤害，或是对环境产生主要的危害	
重大	单一致命性的，或是单个严重伤害，或是对环境产生重要的危害	主系统失效
次要	少许损伤或对环境有一定影响	系统的重大损害
轻微	可能有轻微损伤	系统小的损害

表3 质量风险分级

风险种类	对各种风险采取的对策
不能容忍	应该消除
不希望	当风险减少无法实施时，经铁道或安全主管部门批准后方可接受
可接受	采用适当控制，并经铁道主管部门批准后可以接受
可忽略	可不经铁道主管部门批准就接受

表4 风险评估矩阵的例子

危害事件出现的频度	风险种类			
频繁	不希望	不能容忍	不能容忍	不能容忍
经常	可接受	不希望	不能容忍	不能容忍
有时	可接受	不希望	不希望	不能容忍
很少	可忽略	可接受	不希望	不希望
极少	可忽略	可忽略	可接受	可接受
几乎不可能	可忽略	可忽略	可忽略	可忽略
	轻微	次要	重大	特大
	危害的严重等级			

由表4可见，对于能引发重大或特大事故的故障出现的频度必须是极少级，否则很难被运行部门接受。

IEC 62278给出了风险评估的框架，但仍缺少可操作性，因为它对危害事件出现的频度虽然分成了6级，但没有量化；对危害的严重等级虽然分成了4级，但也没有作出具体界定。而对不同的系统或产品，频度的量化指标以及可能引发的事故严重等级也不尽相同。因而有必要针对机车车辆上的电子产品对标准进行细化，这样才能便于贯彻实施，才有可操作性。

3 机车车辆电子产品的RAMS

3.1 电子产品的故障形式

系统的正常功能可能因为一个不希望事件UE(Unexpectant event)而被破坏，出现不希望事件的原因可能有物理的、逻辑的、信息的和外部的4个论域，发生在物理域的UE称为失效，而从逻辑域到外部域的UE称为故障、差错和错误。由于逻辑域变量只有2个值：正确或不正确，分析起来比较简单，因此最好把其他论域中的UE，归纳在简单术语“故障”之下，尽量用逻辑域来描述。电子产品的故障形式有以下5种：

永久故障：由元件中不可逆变化引起的，它永久地将原逻辑变成一个新逻辑。

瞬时故障：持续时间不超过一个确定的最大时间长度的故障。这类故障只引起有关元件当前值的改变，但不导致不可逆变化。这一般由外部干扰而引起。

间歇故障：是由元件失效，不正确设计或恶劣环境所引起的，但只有若干逻辑变量组合时才发生这类的故障。

物理故障：由物理系统内部的或外部的原因引起，发生在逻辑域的故障。

人为故障：由设计人员的不正确设计和操作人员的误操作而引起的故障。

目前电子产品的故障统计以更换插件或其他重要器件为依据，把更换一个插件作为一次故障看待。这种统计方法可能忽略了瞬时故障和间歇故障，因为回库后，引发这类故障的条件不一定具备，库内检查不出来。实际上在运行中只要有适当的保护措施，复位后也不致影响列车的运行。而采用以更换插件作为故障的统计方法是直观易行的，可以在相当程度上反映产品的质量，由此得到的实际平均无故障时间(AMTBF)可以作为衡量危害出现频度的依据。

3.2 危害出现的频度

《IEC 61508-1——电气/电子/可编程电子安全相关系统的功能安全》第1部分：一般要求中，对安全完整性级别(SIL)作出了规定，它是用执行所要求功能的平均故障率表示的，见表5。

现在机车车辆电子产品的平均故障率一般都属于低要求模式的第3级，个别产品能达到低要求模式的第4级。

这种分级方法是以10的倍数进级的，仍然不够具体，缺少可操作性，而且也无法与IEC 62278中的6个等级相对应。

表5 安全完整性级别

安全完整性级别	执行所要求功能的平均故障率
低要求模式4	$\geq 10^{-5} \sim <10^{-4}$
低要求模式3	$\geq 10^{-4} \sim <10^{-3}$
低要求模式2	$\geq 10^{-3} \sim <10^{-2}$
低要求模式1	$\geq 10^{-2} \sim <10^{-1}$
高要求模式4	$\geq 10^{-9} \sim <10^{-8}$
高要求模式3	$\geq 10^{-8} \sim <10^{-7}$
高要求模式2	$\geq 10^{-7} \sim <10^{-6}$
高要求模式1	$\geq 10^{-6} \sim <10^{-5}$

实际平均无故障时间(AMTBF)与计算的平均无故障时间(MTBF)有着本质的区别。MTBF是在比较理想的条件下计算的,而实际运行条件比较恶劣,振动、冲击、环温变化、发热、坡道、电磁干扰等都会引发故障或缩短使用寿命。AMTBF是根据实际运行中发生故障的次数统计计算得到的,较为客观地反映了实际情况。

对于危害出现的频度进行量化是很困难的,根据个人经验提出下列建议,采用2倍进级的算法:

频繁:每季度都要发生1次或几次;

经常:一季度以上发生1次;

有时:半年以上发生1次;

很少:1年以上发生1次;

极少:2年以上发生1次;

几乎不可能:4年以上发生1次。

如果每天运行16 h,一个月运行26天,一个月的工作小时为416 h,一个季度为1 248 h,圆整为一季度工作1 250 h,则有

频繁	AMTBF<1 250 h
经常	2 500 h>AMTBF≥1 250 h
有时	5 000 h>AMTBF≥2 500 h
很少	10 000 h>AMTBF≥5 000 h
极少	20 000 h>AMTBF≥10 000 h
几乎不可能	AMTBF≥20 000 h

我们目前电子柜的AMTBF一般大于5 000 h,属很少级;SS_{6B}机车电子柜在株洲机务段AMTBF达到15 000 h(属极少级)。但也有的车型如SS_{4B}在运行初期只能达到3 000多小时(属有时级),这主要是由于初期运行电子产品故障的浴盆效应所致,随着时间推移,AMTBF也随之提高。

由于我们产品的AMTBF还不够高,因而从风险评估来说我们的产品不允许引发重大故障或特大故障。另外我们产品的AMTBF大部分还停留在6 000 h左右,要想提高到8 000~10 000 h时,还任重道远,需作出艰苦不懈的努力。

3.3 危害的严重等级

电子产品故障对列车造成的危害大致上可分为:

特大:引发火灾、列车超速、冒进信号;

重大:机破;

次要:由于牵引力/制动力的部分损失造成列车晚点或短时途停,客车空调无电源及故障,造成人身不舒服,门失灵造成上下车不便;

轻微:不造成列车晚点和影响舒适的临修和碎修。

上面这样分类是从严要求的。机务部门把只是由于机车车辆破损而造成的机破事故才算作故障。严格说来,列车在区间非正常停车或在车站内非正常停车超过30 min以上或由于车钩破损而造成的列车分离均为故障。这里把机破归为重大等级。

一个系统或一个产品的故障可分为2种类型:一种是不影响安全的故障,另一种是有危险性的故障。所有电子产品都必须考虑防火措施,如采用足够截面的阻燃导线,防止由于短路电流引发火灾。另外应采取措施防止事故的扩大,单一产品的故障不应影响列车的运行。

机车车辆上的电子产品按功能大致可分属于以下几个系统,有的产品可同时用于几个系统:

空气制动控制系统,如BCU,各种电空阀;

牵引/电制动控制系统,如电子柜,电流、电压、速度传感器;

辅助系统,如辅助变流器的传感器和控制设备;

列车网络显示系统,如网关、节点、显示屏;

列车供电系统,如集中整流分散逆变的传感器和控制设备;

列车监测信息系统,如TIS列车信息系统;

门、空调及照明等的控制设备。

空气制动失灵有可能造成特大事故;牵引/电制动部分功能丧失会造成列车晚点,全部丧失会造成机破;辅助系统故障会造成牵引力/制动力部分或全部丧失;列车网络显示系统故障可造成牵引力/制动力部分损失,影响列车运行速度;列车供电系统及门、空调、照明的故障会使人身环境条件恶化和造成旅客上下车的不便;列车监测信息系统一般不参与列车控制,不会直接影响列车安全或列车晚点。

ATP是防止超速冒进的安全设备,应具有相当可靠性。ATP失效时应及时告知司机改自动驾驶为人工驾驶,从而使它的故障影响减少,但可能造成列车晚点。

各个产品应具体分析,按其故障引起后果的严重性,按表4得到它可接受的故障频度。

4 铁道电子产品降低风险的设计对策

降低风险的设计对策主要从冗余设计、故障诊断和可靠性设计3个方面着手。

4.1 冗余设计

一个系统或一个产品的作用决定了它故障时的危害严重程度,而通过冗余设计可以把危害严重程度降低1级甚至2级。

例如:电力机车上的模拟电子柜控制分成A、B两组,在A组故障时改为B组控制,此时功能不如A组完善,会影响牵引力的发挥,但不会造成牵引力全部丧失和机破。在微机控制的电力机车上,故障位改转向架独

立控制为集中控制，仍可发挥原来的牵引力/制动力，因而不会造成列车晚点。只有当2个转向架的控制同时失效才会造成机破，当然这种故障的几率是极少的。

制动系统事关列车安全。为提高安全性，在“中华之星”高速列车上采用3套制动系统冗余的方案：即以微机控制的直通电空制动为主、基础制动为辅、备用空气制动作为电空制动失效时的保护措施，从而使BCU（制动控制单元）失效时的危害性降低1~2个等级。BCU故障可能影响列车速度的发挥，引起列车晚点，但不会造成人伤械损的特大事故。

冗余会使系统复杂化和成本增加。冗余是否必要，以及系统冗余到什么程度，必须在设计开始时综合分析。冗余采用热备（自动转换）还是冷备（手动转换）也要具体分析，只有自动转换技术成熟时方可用热备，否则宁可采用手动转换。

除通常采用的硬件冗余外，还可在时间、信息和软件上采用冗余。

时间冗余是通过消耗时间资源来达到容错的目标。例如采用程序卷回来检验一般程序完成的计算数据和操作结果，如果有错，则卷回重新执行。

信息冗余是靠增加信息的多余度来提高可靠性。一种是将重要信息送至2个或2个以上的设备，以便在其中一个设备故障时仍能从另一设备取得该项信息。另一种是在信息代码中增加附加信息，以便当代码中的某些信息位发生错误时能及时检错，或是能恢复原来的信息即纠错。

软件冗余是提供足够的冗余信息和算法程序，使系统在实际运行中能及时发现程序错误，采取补救措施，保证系统的正确运行。

4.2 故障诊断

故障诊断的作用是在某个设备故障失效时及时把此信息通知司机，以便司机采取相应措施，从而防止重大事故的发生和缩小故障范围。此外通过故障诊断指明故障损坏的部位和当时的工况，以便找出故障原因和缩短维护时间。

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

《IEC 61508-2 电气/电子/可编程电子安全相关系统的功能安全》第2部分：电气、电子、可编程电子安全相关系统的要求，对系统的安全故障率有明确的规定：对于SIL3（SIL为安全完整性级别）系统，安全故障率应在90%~99%，而对危险性故障的诊断覆盖率也应达到90%。

目前我们的故障诊断还处于较低的水平，要达到上述的诊断覆盖率还需做大量的工作。对于高速列车，在轮对轴承机械方面的检测也是一项非常紧迫的任务。

4.3 可靠性设计

图2是产品可靠性设计流程图。

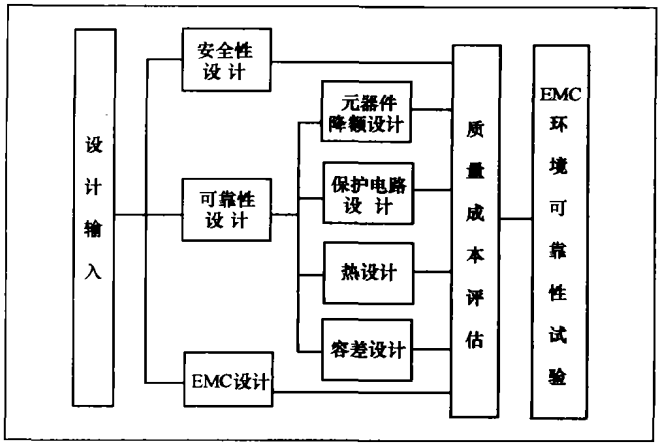

图2 产品可靠性设计流程图

提高车载微机的可靠性主要有2种方法：一是“避错”，就是用正确的理论指导设计及严格工艺质量控制，尽量避免故障或故障产生的条件；二是“容错”，当发生某些硬件或软件故障时，系统能执行一组程序，使系统不会发生严重的操作错误，过程仍能进行或降功运行。图2中的元件降额设计，热设计主要是避错，而保护电路设计及容差设计，则主要为容错。冗余设计和故障诊断主要是容错，而EMC设计既有避错又有容错的措施。关于可靠性设计已经在许多论文和书籍中论述，这里不再赘述。参见文献3、4。

5 结束语

（1）本文从实际应用出发，提出按实际平均无故障时间（AMTBF）来量化事故出现频度的等级，具有可操作性，既符合当前实际情况，又能促使产品质量的提高。

（2）机车车辆上的各种电子装置故障时所引发的事故严重等级是不等同的，因此在产品设计时，可按照它的重要程度分别采取对策。

（3）为减少电子产品故障时的风险，应采取冗余设计、可靠性设计和故障诊断。尤其是故障诊断，在系统设计时应特别予以重视。

参考文献：

[1] IEC 62278：2002， 铁路应用——铁道可靠性、可用性、可维护性、安全性（RAMS）规范及说明[S].

[2] IEC 61508：1998，电气/电子/可编程电子安全相关系统的功能安全[S].

[3] 蒋兆远.车载微机的可靠性研究[J]. 兰州铁道学院学报（自然科学版），2001,(4).

[4] 李宗亮.电子可靠性设计与成本控制[J]. 电子产品可靠性与环境试验，2002,(2).