高等学校教学参考书

铁路信号容错技术

上海铁道大学　员春欣　主编

北方交通大学　吴运熙　主审

中　国　铁　道　出　版　社

1997年·北京

前　言

在铁路信号设备微型计算机化的进程中，综合采用各种容错技术提高计算机系统的可靠性和安全性，以满足铁路运输现代化的要求，这是世界各国发展铁路信号高新技术的必由之路。为适应这一技术发展潮流，于80年代初，我在上海铁道大学为铁路信号专业的本科生、研究生开设了《铁路信号容错技术》课。在近十次教学实践的基础上，吸取了从事容错技术科研的体会，三次易稿，编写出《铁路信号容错技术》讲义。根据铁路高校通信信号教学指导委员会1993年8月的决定，委托我主编《铁路信号容错技术》选修课教材。此后，又经过加工修改，在各方面的大力支持下，该书终于呈献给读者。

本教材围绕铁路信号设备用微型计算机系统的高可靠性、高安全性要求，并密切联系采用微型计算机的铁路信号设备的实例，仔细进行选材。着眼于容错技术的基本概念、基本知识和基本技术理论，并突出故障安全技术，这就是编写本教材的指导思想。

由于铁路信号专业教学计划设置了《可靠性工程》、《编码理论》等课程，所以本教材不包括信息冗余技术和容错系统的可靠性评价等内容。

全书包括四部分内容：总论，故障测试，资源冗余及其管理，故障安全技术。全书分为九章，依次为：铁路信号容错技术总论（加强了故障安全技术概论），故障测试（侧重在线功能测试），硬件冗余（侧重二模冗余）技术，软件冗余技术（加强了软件容错，或者说软件抗干扰技术），故障安全组合逻辑电路，故障安全时序逻辑电路，自校验逻辑电路，故障安全计算机，软件系统的故障安全。

全书内容的编写是我和周治邦副教授长期合作、共同耕耘的结果，在执笔完稿时作了具体分工。第六章、第九章、第二章中的微处理器的功能测试、交替逻辑技术、永久性故障和瞬时性故障的判别等内容由周治邦执笔编写，余下内容由我执笔完稿。

全书由北方交通大学吴运熙教授主审。上海铁道大学吴芳美教授、兰州铁道学院姚昆岚教授对本书提供了许多宝贵意见。上海铁道大学的缪润生副教授曾审阅了本书的第三稿，并提出了许多建议。作者向各位先生深表谢意。

主编 1997,8 于上海

（京）新登字 063 号

内 容 简 介

本书围绕铁路信号用的微型计算机系统的高可靠性、高安全性的要求，以容错技术的基本概念、基本知识和基本技术理论为基础，以故障安全技术为主线，详细阐述了故障测试、硬件冗余技术、软件冗余技术、故障安全组合逻辑电路、故障安全时序逻辑电路、自校验逻辑电路、故障安全计算机、软件系统的故障安全等内容。

本书为高等学校自控专业研究生教材或教学参考书，也可供自控专业的工程技术人员学习参考。

图书在版编目(CIP)数据

铁路信号容错技术/员春欣主编. -北京：中国铁道出版社，1997
高等学校教学参考书
ISBN 7-113-02634-6

Ⅰ. 铁… Ⅱ. 员… Ⅲ. 铁路信号-容错技术-高等学校-教学参考资料 Ⅳ. U284.15

中国版本图书馆 CIP 数据核字(97)第 11565 号

高等学校教学参考书
铁路信号容错技术
上海铁道大学 员春欣 主编
*
中国铁道出版社出版发行
（北京市宣武区右安门西街 8 号）
责任编辑 倪嘉寒 封面设计 赵敏宇
各 地 新 华 书 店 经 售
中国铁道出版社印刷厂印刷

开本：787×1092 1/16 印张：13.5 字数：326 千
1997 年 10 月 第 1 版 第 1 次印刷
印数：1—2000 册

ISBN7-113-02634-6/TN・101 定价：21.80 元

目　录

第一章　总　论 …… 1
1.1 容错技术概论 …… 1
1.2 故障安全技术概论 …… 7
第二章　故障测试 …… 20
2.1 数字电路(或系统)的故障和故障模型 …… 20
2.2 故障测试总论 …… 27
2.3 部件的功能测试 …… 30
2.4 门级的结构测试 …… 45
2.5 其它的故障检测技术 …… 56
2.6 系统级诊断 …… 60
第三章　硬件冗余技术 …… 67
3.1 冗余技术的基本概念 …… 67
3.2 N 模冗余技术 …… 68
3.3 待命储备系统 …… 78
3.4 混合冗余系统 …… 79
3.5 二模冗余系统 …… 80
3.6 局部网络冗余技术 …… 90
第四章　软件冗余技术 …… 97
4.1 软件可靠性的基本概念 …… 97
4.2 软件的避错技术 …… 100
4.3 容错软件的结构 …… 102
4.4 软件错误检测技术 …… 107
4.5 软件容错技术 …… 109
第五章　故障安全组合逻辑电路 …… 119
5.1 基本故障安全逻辑电路的定义 …… 119
5.2 单调逻辑函数 …… 119
5.3 基本故障安全逻辑电路的条件 …… 121
5.4 故障安全组合逻辑电路 …… 122
5.5 实现基本故障安全逻辑电路应该考虑的主要问题 …… 122
5.6 电阻一晶体管调变式故障安全逻辑电路 …… 124
5.7 三值故障安全逻辑电路 …… 125
5.8 交替逻辑电路及其故障安全性 …… 128
第六章　故障安全的时序逻辑电路 …… 131
6.1 时序电路和状态机 …… 131

6.2 故障安全(FS)时序电路基本概念 …… 137
6.3 用对称出错元件(SFE)和波格码设计 FS 同步时序电路 …… 141
6.4 用对称出错元件(SFE)和等重码$_nC_n$设计 FS 同步时序电路 …… 148
6.5 用 SFE 元件和集合分划理论设计 FS 同步时序电路 …… 151
6.6 N-FS 时序电路 …… 155
第七章 自校验逻辑电路 …… 160
7.1 概 述 …… 160
7.2 自校验逻辑电路的特点及一般结构模型 …… 160
7.3 自校验逻辑电路的定义 …… 161
7.4 完全自校验检测器 …… 164
7.5 双轨代码完全自校验检测器 …… 165
7.6 奇偶校验码完全自校验检测器 …… 166
7.7 m/n 编码的完全自校验检测器 …… 167
7.8 强故障保险逻辑 …… 169
7.9 自校验和故障安全的关系 …… 169
第八章 故障安全计算机 …… 170
8.1 概 述 …… 170
8.2 铁路信号设备微型计算机化的特点 …… 172
8.3 单机闭环自诊断故障安全计算机 …… 173
8.4 采用单机软件冗余的故障安全计算机 …… 174
8.5 双模紧密耦合总线同步式故障安全计算机 …… 176
8.6 双模时差同步式故障安全计算机 …… 178
8.7 双模软件冗余的故障安全计算机 …… 180
8.8 三模紧密耦合总线同步式故障安全计算机 …… 182
8.9 三模松散耦合式故障安全计算机 …… 186
8.10 故障安全输入接口 …… 186
8.11 故障安全输出接口 …… 188
8.12 故障安全传输 …… 190
第九章 软件系统的故障安全 …… 192
9.1 软件系统故障安全概述 …… 192
9.2 软件故障安全性需求分析 …… 193
9.3 软件系统的故障安全性设计准则 …… 196
9.4 软件系统安全性验证和评估 …… 203
主要参考文献 …… 206

第一章 总 论

电子计算机在各个领域的广泛应用，尤其是铁路信号设备的微型计算机化，计算机系统的可靠性、安全性成了一个重要的指标。采用避错和容错两种技术可以有效地提高计算机的可靠性、安全性。尤其是容错技术，它是构造高可靠性高安全性计算机系统的有力手段，也是当今最活跃的一个研究领域。为了使读者对容错技术的全貌有一概括的了解，本章讨论以下几个问题：容错的含义和定义，容错技术的主要内容，容错技术的重要性，故障安全技术概论。

1.1 容错技术概论

1.1.1 容错的含义和定义

容错这个词是从英语"*Fault-Tolerance*"一词翻译过来的，该词原义是"抗故障"或"耐故障"。中文译词却取"*Tolerance*"词条中的第一个词义"容许、容忍"，而"*Fault*"又译成错误，故两词合一便译成"容错"，即是"容忍错误"之意。对于任意一个系统而言，都希望在内部出错的情况下，系统的功能仍能保持正常。因此，容错是一个具有广泛意义的概念。我们将侧重计算机的容错技术，简称容错计算技术(*Fault-Tolerant Concputing*)。现在我们就来阐述容错计算的含义。

"计算"一词的含义，在今天已经远远超出数值计算的范围。一般来说，计算机能够做的工作都可以叫"计算"，它包含信息处理、过程控制、人工智能等众多领域，而且"计算"所包括的范围还在不断扩大。

"容错计算"是容许某些故障存在的计算。这里的"错"是指"故障"而不是指差错。容错计算不能理解为计算错了也没关系，恰恰相反，它的含义是指在计算机系统的硬件或软件存在故障的情况下，仍然能正确地执行给定的算法。

Algirds Avizienis 在 1972 年发表的《容错计算的方法》和在 1975 年发表的《容错计算机系统的结构》两篇论文中给"容错计算机"作了如下定义：

"一台容错计算机，在计算机系统中出现故障的情况下，能正确地执行它的全部程序组"。这个定义不仅表达了容错计算的确切含义，而且指出了计算机系统和其它物理系统的差别就在于，计算机的"正确运行"是指一组程序的正确执行，而不是指系统的一套元件的连续工作。

只要满足下列四个条件，即构成"正确执行一组程序"的定义，或者说正确的执行程序用下而四个标准来判断：

1. 程序及其数据不为故障所改变或中止；
2. 运算的结果不包含由故障所带来的差错；
3. 每个程序的执行时间不超过某一规定的限界；
4. 每个程序可利用的存储容量保持在某一规定的最小值之上。

程序组和数据、所需运算的定义、程序执行的时间限制和存储容量的要求，由系统的总体设计人员和用户共同提出。设计人员的目标是在程序执行期间可能发生故障的条件下，把系统的可靠性提高到可以接受的高数值。

1.1.2 容错技术的重要性

从电子计算机诞生之日起，电子计算机的可靠性就实实在在地摆在了人们面前，这是来自应用实践的要求。随着电子计算机应用范围的日益扩大，囊括了许多极其重要的领域，尤其电子计算机在整个地球上辽阔的地理分布及其在宇宙空间的应用，电子计算机的可靠性变得越来越重要。概括起来有以下几方面的原因：

1. 随着电子计算机功能的日益完备和运算速率的提高，其组成日趋复杂，所使用的元器件日益增加，装配密度日益加大，主振频率也日益提高，这都将使电子计算机系统发生故障的概率增大。为了使系统的可靠性不随性能的提高而急剧下降，必须进行精心的可靠性设计。

2. 随着电子计算机走向广阔的领域，为各行各业所应用，电子计算机的操作使用者不再只是计算机专业人员，这就要求电子计算机系统必须能够防止或容忍人为的操作失误。

3. 由于电子计算机系统的应用日益广泛，电子计算机的使用环境将不只是有空调、屏蔽、无冲击、无振动的试验室，而是一个恶劣的运行环境，如高低温、高湿度、沙尘。电磁干扰、机械冲击和振动、盐雾、霉菌、辐射等加于电子计算上，使电子计算机更容易出错。这就要求电子计算机具有抗恶劣环境的能力。

4. 随着大规模集成电路和超大规模集成电路的社会化大生产，使得电子计算机硬件的研制和生产成本日益降低，而维护使用的成本相对提高。这就要求通过提高电子计算机系统的可靠性，减小发生故障的概率，以降低维护使用成本。

5. 随着电子计算机的普及，社会对它的依赖性越来越强，如果计算机出错可能造成重大损失，甚至酿成巨大的灾难。因此，也需要高可靠性的计算机。

为了提高计算机系统的可靠性，在长期使用电子计算机的实践中，使用并发展了基本原理不同的两种保证技术：避错技术和容错技术。

避错技术的目标就是尽量减小系统发生故障的概率，也就是从尽量减小系统的失效率入手达到提高系统可靠性的目的，它是提高计算机系统可靠性的必不可少的常规方法。

影响计算机系统可靠性的因素可以归纳为内部因素和外部因素。内部因素主要是指组成计算机系统的硬件和软件的内在质量，外部因素主要是指应用计算机的外部环境条件。因此，避错技术主要包括质量控制技术和环境防护技术两大部分内容，下面对此作一简要介绍。

质量控制技术。由于元器件是构成计算机系统的基础，可以说对系统的可靠性有着决定性的影响。因此，在计算机系统的研制过程中，应认真实施元器件工程，加强对元器件的选择、使用和管理。在此基础上，对组装工艺实行严格的质量管理规范。此外，还必须认真实施软件工程，以保证软件的内在质量。这些措施，是生产出高可靠性计算机系统的有效的强有力的保证。

环境防护技术。随着计算机的普及，计算机已从具有良好环境的机房迁移到各种应用现场。各种环境因素施加于计算机上，使计算机更容易出错。必须采用适当的环境防护技术，如热设计技术、机械应力防护技术、化学防护技术、电磁兼容性设计技术等，使计算机系统具有抗恶劣环境的能力，这也是提高计算机系统可靠性的重要途径。

虽然避错技术是提高计算机系统可靠性的必不可少的有效措施，但它并不能完全解决计算机系统的可靠性问题。原因如下：

1. 避错技术的目标是尽量减小系统发生故障的概率。实践证明，这种减小是有一定的限度的，超过这个限度再进一步降低就要付出巨大的投资，有时甚至是很困难的。这是由于降低元器件的故障率除了受到元器件材料的限制外，还受到当时的生产技术条件、生产工艺水平等的

限制，并受运行环境的制约。

2. 既然避错技术只能使故障率减小，但永远不可能使硬件、软件的故障率减为 0，因而计算机系统的故障发生是不可避免的，系统的失效也是在劫难逃。

3. 避错技术对故障的处理均由系统外部提供，在计算机硬件成本日益降低的情况下，使计算机的维护成本相对提高。不仅如此，一旦计算机系统发生失效，对某些实时系统（如航天飞机、卫星控制等）不能像一般的系统那样，可以立即由人维修恢复正常运行，由此可能造成严重的经济损失，甚至是灾难性的后果。

由此看来，避错技术在提高计算机系统可靠性上是有局限性的。为此，要进一步提高计算机系统的可靠性还必须采用容错技术。

容错技术是以承认故障的不可避免性为前提的，也就是在容忍故障存在的条件下提高计算机系统可靠性的措施。

这里需要强调指出，尽管容错技术可以实现系统的超高可靠性，但并不能用容错技术完全代替避错技术。容错技术应看作是避错技术的重要补充。在设计系统时，应该首先采用避错技术，使其具有较高的可靠性。在此基础上，再综合使用各种容错技术，使系统的可靠性在较低的费用下达到设计的目标。如果原始系统本来就是可靠性不高，此时采用容错技术所能起的作用就很小，在设计不当的时候，甚至效果更坏。

1.1.3 容错技术的主要内容

从 1952 年冯·诺依曼（Von·Neuman）在美国加里福尼亚理工学院作了五个关于容错理论研究的报告，奠定了容错技术的基础以来，容错技术已发展成为独立的学科，其内容越来越丰富。但就其具体技术而言可以概括为三大部分：

一、故障测试

故障测试是容错技术的主要组成部分，又是微电子技术的支撑技术，因而形成了一个独立的学科。

回答一个系统是否存在故障的过程称为故障检测（*fault detection*），回答一个系统在哪里发生了故障的过程叫故障定位（*fault location*），故障检测和故障定位合称为故障测试（*fault testing*），又称故障诊断（*fault diagnosis*）。

故障测试技术主要包括：测试集生成技术，功能测试技术，可测试设计技术，自校验技术，系统诊断技术等。

二、冗余及其管理技术

容错计算是依靠计算机资源的冗余来实现的，通过合理使用硬件冗余、时间冗余、信息冗余、软件冗余达到提高计算机系统可靠性的目标，可以说它是容错技术的核心。

硬件冗余：在常规设计的硬件之外，再附加备份硬件。硬件冗余包括静态冗余（又称堆积冗余）、动态冗余（又称待命储备冗余）和将两种冗余结合运用构成的混合冗余。硬件冗余可以在元器件级、部件级、模块级、整机级上实现。

时间冗余：重复地执行指令或一段程序而附加额外的时间。

信息冗余：增加信息的多余度，使其具有检错和纠错能力。

软件冗余：用于测试、检错的外加程序，用于计算机系统的自动重组、降级运行的外加程序等。主要包括容错软件和软件容错两方面的内容。

三、故障安全技术

故障安全技术始于铁道信号，并以各个时代的技术水平为背景不断进步和发展起来的。已在航空、原子能、化工、机器人、医疗设备、交通信号、家用电器等领域广泛地使用。它已成为容错技术的重要组成部分。它的主要内容包括：故障安全概念及其发展；以故障安全技术为核心的安全技术体系；故障安全逻辑理论、电路和部件；故障安全编码理论；故障安全计算机结构理论；故障安全软件的理论等。

1.1.4 容错计算技术的发展概况

任何一门科学技术的产生和发展与人类的生产实践和科学实验的发展密切相关的，容错计算技术也不例外。

电子计算机的产生和发展并在各个领域被广泛地使用，如何不断提高电子计算机的可靠性以满足实际使用的要求，就成了推动容错计算技术的产生和发展的原动力。

以大规模和超大规模集成电路为核心的微电子技术的突飞猛进，使得电子计算机的最主要的构成元素—器件可靠性迅速提高，并且由于它的小型化、价格便宜，对容错计算技术的导入，减少了技术、经济上的阻力。不仅为电子计算机系统的高可靠性打下了坚实的物质基础，并对容错计算技术的发展起到推动作用。

以概率论和数理统计为基础的可靠性理论的形成和发展，对容错计算技术的发展起到了指导作用，推动了容错计算技术的体系化和理论化。

基于上述，首先我们以容错计算机的发展为主线，对容错计算技术的发展作一扼要的历史回顾。

一、容错计算技术的开创阶段

1951 年 3 月，在冯·诺依曼领导下的研究小组把第一台 UNIVAC-Ⅰ电子计算机交付美国人口统计局使用，揭开了电子计算机实际应用的帷幕。UNIVAC-Ⅰ不仅凝聚了冯·诺依曼的"存储程序"的思想，而且充分展现了他的可靠性设计思想。UNIVAC-Ⅰ最先采用了奇偶校验码和以匹配一比较方式工作的双重运算线路，从而保证了系统的可靠性。1951 年到 1956 年共生产了 20 台 UNIVAC-Ⅰ，用于军事、科研、管理等方面。

1952 年冯·诺依曼在加利福尼亚技术学院作了关于容错理论研究的五个报告，他分析了人脑处理错误数据的情况，提出了修补器官的概念，他指出，人脑工作的可靠性是由结构上较低一级的冗余来保证的。1956 年他又证明：通过容错技术可以用较不可靠的器件组成可靠的系统。

可以说，冯·诺依曼的实践和理论奠定了容错计算技术的基础。

二、早期的容错计算机系统

第一台容错计算机是于 1954 年在捷克斯洛伐克建成的，取名叫 SAPO。在 SAPO 系统中，三模冗余和表决技术用于并行的 *CPU* 中，在存贮器中使用了奇偶校验和比较手段。发现错误时可进行自动重试或自动停机。世界上第二台容错计算机也是捷克斯洛伐克制造的。

第二代晶体管计算机的问世，由于它采用了可靠性高的半导体管和磁芯为主要元件，使计算机的可靠性大大提高，而冗余硬件和故障恢复机构又使系统的成本增加很多，从而使自动故障恢复不再被认为是合算的，此时，重点放在设计时采用故障检测机构，提供完善的诊断手段。60 年代中期，出现了很有效的测试组合电路的算法，最著名的是 D 算法。此时，开始采用微程序设计，用微码写诊断程序，对内部逻辑可进行更有效的测试和诊断。故障检测逻辑、单条指令

的重试以及微诊断已用在许多计算机中。

三、60 年代的专用容错系统

美国早期的容错计算机是在 60 年代为空间计划和电话公司开发的。

由于载人飞行的航天器和发射系统要有极高的可靠性，因而美国航空航天管理局(NASA)是容错计算机研制开发的主要支持者。

美国航空航天局支持的第一台容错计算机是轨道天文观测台(OAO)、卫星用的星载计算机。OAO 计算机建于 1961～1965 年，可靠性指标要求在一年运行期中可靠率为 95%。所采取的主要容错技术如下：

1. 该机采用分离的晶体管元件，在串并联电路中用四个晶体管代替原来的一只晶体管，如果任一晶体管失效，其它 3 个可以继续工作，提供正确的逻辑功能；

2. 存贮单元实行三模表决、数据双份存贮，命令则是四份。

美国航空航天局支持的第二台容错计算机是阿波罗登月飞船的制导计算机，它建于 1962～1969 年，可靠性指标是在 250h 运行时间内可靠率为 99%。所采用的容错技术如下：

1. 它采用三模冗余(TMR)工作方式.三个处理器运行相同的程序，对结果进行表决，它可屏蔽任何单个处理器的故障。

2. 采用两个磁心存贮器，同时写相同的数据，并且用错误检测码编码，如果某一个存贮器出现故障，该存贮器的数据编码就会出现错误，此时处理器将使用另一个存贮器中的数据。

阿波罗制导计算机的研制成功是容错计算机系统发展史上的一个里程碑，为以后美国航天飞机用的容错计算机系统的研制奠定了基础。

美国航空航天局支持的第三个容错计算机是喷气推进实验室(JPL)的自测试自修复(STAR)计算机。它是为深空间任务而开发的，运行寿命至少 10 年，STAR 计算机是在 A·Avizienis 领导下设计的，于 1969 年在加州理工学院建成的，所采用的容错技术如下：

该计算机由若干存贮器、一个运算处理器、一个控制处理器、一个 *I/O* 处理器和一个测试与修复处理器组成。每个部件在运行正常程序的同时检测自身内部的故障并发出信号。测试与修复处理器专门负责测试与修复的处理，它监测系统其余部件的运行，接收故障报告，并可进行重组与修复。

该计算机采用混合冗余结构，以三模表决方式工作，并有多个备份部件。

STAR 计算机进行了试验与测试，但由于美国航空航天局取消了原计划而未投入使用。尽管如此，它对容错计算技术的发展却做出了重大的贡献。

有 60 年代最广泛使用的容错计算机系统是贝尔电话公司开发的电话交换系统(ESS)。可靠性指标是 40 年的运行期内，系统不能工作的时间不超过两小时。ESS 系统中所有关键部件都是双份的，并设计了许多专门完成故障检测、定位和隔离的硬件和软件，它允许人工进行失效部件的替换，这个系统一直应用到今天。

到 60 年代末，几乎在所有后来设计中所用到的容错基本形式，诸如三模冗余、双仿比较、自校验部件都已形成。

在 60 年代，诞生了故障安全逻辑理论，并得到迅速的发展。关于这方面的内容，将在本章第二节详细叙述。

四、70 年代容错计算技术的发展

70 年代，容错计算机系统又有了较大的发展，出现了许多有重要意义的研究性系统和实用系统。

SIFT 计算机是由美国国家航空航天管理局(NASA)资助,由斯坦福国际研究所(SRI)八位科学家负责研究,BENDIX 计算机公司五人参加工程模型的设计与制造。SIFT 的研究始于1970 年,直到 1980 年才完成实验样机。它是应用于商业飞机的大型飞行控制系统,可靠性目标是在 10h 的运行期中失效率小于 10^{-9}。

由于 SIFT 计算机的可靠性目标是短时间的高可靠运行,因此在硬件设计中采用了 N 模冗余技术,各模块使用独立的时钟。但它的主要特点是首次提出了用软件实现容错(*Software Implimented Fawlt－Tolerance*)的概念,其基本思想是用软件实现同步、表决、故障的隔离、错误的检测、错误的分析以及系统的重组。

与此同时,在美国航空航天管理局资助下,由麻省理工学院的 Draper 实验室开发了 FTMP(Fault-Tolerant Multiprocessor)计算机。它也是应用于商业飞机的大飞行控制系统,可靠性目标是在 10h 的运行期中失效率小于 10^{-9}。

FTMP 基本上是一个硬件容错计算机,是一个复杂的多处理器计算机,它使用与 *TMR*—混合冗余有关的冗余形式,它有一个硬件实现的高可靠容错时钟,它可以容忍时钟本身的故障,以保证各处理机的严格同步,并用硬件实现表决。

容错计算机系统从特殊的应用领域走向一般的应用领域,从科学研究走向商品化,是容错计算机系统的一个重要的进展。在 70 年代末,出现了为商用目的进行开发的 Intel432 计算机和 Tandem-Nonstop 系统。Intel432 计算机由于设计复杂、价格昂贵、使用不方便未得到广泛应用。而美国 Tandem 公司的不停顿系统,70 年代末投入使用,80 年代得到了广泛的应用,主要用作联机事务处理。

除了容错计算机系统自身的迅速发展外,在一般通用计算机中也广泛地采用容错技术。IBM 公司的 308X 系统和 4300 系列,Cray 公司的 Cray-1,DEC 公司 VAX-11 系列,Honeywell 公司的 Level/Dps 系列等都不同程度地采用了检错/纠错码、重试、自校验和恢复、维护诊断处理器、多机体系结构等容错技术。容错成为当代计算机系统不可缺少的重要功能。

五、80 年代容错计算技术的发展特征

1. 商用容错计算机市场的出现。以前的容错计算机系统基本上都是结构比较特殊、专用性很强的系统,由于容错的代价过大,限制了容错系统的应用。

进入 80 年代,VLSI 技术的发展,使计算机硬件成本大大降低,平均每年下降 20%以上。同时,计算机进入社会的各个领域,人们对计算机的依赖越来越大,在许多场合,计算机的故障会带来巨大的损失。这就使得商用容错计算机系统应运而生,容错计算机从军事、航天等部门逐步扩大到工业控制、实时系统和联机事务处理(主要是银行、交通部门)等领域。下面举出几家生产容错计算机的公司及其主要产品系列:

Tandem Computer 公司 70 年代末推出了 Tandem-Nonstop(不停顿)系统,90 年代推出 IntegrityS_2 系列。

Stratus Computer 公司推出 FT-250 系列,XA-2000 系列。

IBM 公司的 308 系列和 4200 系列。

DEC 公司的 VAXft3000 系列。

2. 分布式容错计算机系统。多机分布式系统结构是模块化的,计算机的数目是可变的,这些计算机均有自己的局部存储器和外部设备,它们既可独立的工作,也可并行合作,彼此间的通信是经由通信链路的消息交换来完成的。这些分布式系统在物理上是松散耦合的多机系统,而在逻辑上是紧密耦合的多机系统。

分布式容错系统中若有一个或几个计算机或通路发生故障时，其余部分仍可重构成一个新的系统，它仍可以工作，甚至可以继续其失效部分的部分或全部工作，这称为优美降级。当故障排除后，系统又自动恢复，这种优美降级和自动恢复就是系统的健壮性，这是分布系统在容错能力上的特点之一。

此外，分布式系统提供了冗余计算的环境，可以让一个任务在多个处理模块上独立地、并行地执行(称为仿作)，而且同一时间允许多个任务同时仿作。仿作可以根据所执行任务的重要性、实时性的要求是一重、二重或多重的。多重仿作通过表决选择正确结果送出系统，这是分布式系统在容错能力上的又一表现。

3. 容错的 VLSI 技术。对半导体器件的可靠性进行实验分析的结论为芯片的失效率是其复杂程度的函数，即 VLSI 芯片的失效率是 LSI 芯片失效率的 100 倍。所以必须开发具有容错功能的 VLSI。如将动态冗余技术用于 VLSI 设计，产生了所谓的可重构 VLSI；还有一种在 VLSI 上实现自校验逻辑的方法，实现自校验比较。用 PLA 进行容错设计是实现硅片容错的另一途径。

4. 人工智能在容错技术上的应用—计算机故障诊断专家系统。计算机故障诊断专家系统，就是根据专家提供的故障检测与诊断领域的知识构成知识库，借助推理机构，根据系统出故障时的现象，进行精确推理和不精确推理，对故障进行检测和定位。这样就可以使普通的工程技术人员加快故障诊断的过程。

1.2 故障安全技术概论

1.2.1 故障安全概念

故障安全是安全工程学中最基本最重要的概念之一。它最早产生于铁路信号控制领域。随着工业化大生产的发展，安全生产日益成为社会普遍关注的问题，故障安全概念逐渐扩展到核工业、航空航天工业、石油化学工业、公路交通控制、医疗仪器、家用电器等领域，促使故障安全概念更加丰富。随着科学技术的进步，其中以微处理器为核心的微电子技术的日益月异，为故障安全系统提供了价格低廉的先进的物质基础；以微型计算机为主体的容错计算技术的形成和发展，为安全系统提供了先进的系统结构手段；以概率论为基础的可靠性理论的建立和普及，为安全系统的评价提供了有效的理论武器。所有上述一切，对故障安全概念认识的深度和广度都产生了巨大的影响，推动从古典安全概念向近代故障安全概念的转变。伴随着这个转变过程，使安全工程学朝着现代化的目标迈进。由此看来，讨论故障安全概念的演变，深刻认识故障安全概念的特性有着多么重要的意义。

一、故障安全概念的绝对化和它的概率性

铁路信号的基本作用之一就是保证列车、车列运行的安全，而这种安全的实现又总是把“系统故障时让列车停止”作为第一条件。随之也相应地规定：系统故障时把信号显示变为让列车停止的红灯为安全侧。这是传统的铁路信号故障安全技术的一个重要特点。

由于驾驶机车的司机对信号显示的百分之百的信任和无条件的绝对服从，一旦信号设备发生故障、信号机出现错误显示将造成巨大的生命、财产上的损失。历史上血的教训，促使人们形成了要绝对保证安全的指导思想：为了保证列车运行安全，在信号设备发生故障时，绝对禁止向显示“进行信号”的危险侧动作，而必须倒向“显示停止信号”的安全侧。这就是故障安全一词所具有的直观含义。

在既有信号设备中，故障安全的实现又是以具有非对称错误特性的信号继电器和闭路原

理为基础，实现信号设备的整体性的故障安全。这是既有铁路信号安全技术的第二个特点。由于这种继电器的非对称错误特性主要是借助永恒的重力实现的。因而人们认为：在任何故障情况下必定倒向安全侧，具有百分之百的安全性，从而把它叫做安全型继电器。这就进一步加深了故障安全概念的绝对化。

这种绝对化的故障安全概念对铁路信号设备的发展起着极大的阻碍作用。一个时期，尽管半导体器件早已成功地用于各种领域，但由于它不具有非对称错误特性，怀疑它能否组成具有故障安全特性的信号设备，因而不敢或不愿把它在铁路信号设备中广泛应用，使电子技术和控制论在铁路信号中的推广受到影响。

随着可靠性理论的诞生和发展，促使对故障的分析建立在概率论的科学基础上，进而揭示了故障安全也应是一个具有概率特性的概念。具体说，它包含以下内容：

1. 客观上可靠度为百分之百的铁路信号设备是不存在的，也就是说设备的故障是不可避免的，用全故障率 λ_t 表示，希望它足够小。

2. 对设备的故障根据它带来的后果可以分为危险侧故障和安全侧故障，分别用危险侧故障率 λ_d 和安全侧故障率 λ_s 表示，且有

$$\lambda_t=\lambda_d+\lambda_s \tag{1—1}$$

实际上，信号用继电器尽管采取了一系列措施实现故障安全原则，但由于前接点组熔接而发生事故的例子也不是完全没有的。日本的坪井正男氏从过去 20 年间的实际使用结果统计得到信号用继电器的 $\lambda_d=10^{-10}/h$，$\lambda_s=5\times10^{-7}/h$。这表明，危险侧的故障率是比较低的，但不可能等于零，因此故障安全的概念不是绝对的。

3. 在考虑了设备的所有故障的情况下，危险侧故障率 λ_d 相对全故障率 λ_t 小到可以忽略的程度时（但永远不会为 0），该设备才是故障安全的，即危险比 δ 为

$$\delta=\frac{\lambda_d}{\lambda_t} \tag{1—2}$$

δ 应该足够小。

上式还可以写成

$$\delta=\frac{1}{1+\dfrac{1}{\lambda_d/\lambda_s}} \tag{1—3}$$

式中的 $\lambda_d/\lambda_s=\gamma$ 叫做非对称错误率，它应该足够小。

但要注意，我们真正的目标是要 λ_d 的绝对值要小，通过减小 λ_d 来减小 δ 或 γ。否则会造成错觉：尽管 λ_d 并不小，而 λ_s 却大，使得 δ 或 γ 很小，从而把设备看成是故障安全的。

事实上，由于信号设备发生故障时列车停止运行，这样一来，安全侧故障率 λ_s 越大，故障恢复时间越长，越益引起列车的阻塞。这不仅降低运输效率，而且还容易诱发重大事故。因此 λ_s 也应尽可能小。

总之，从故障安全的实现来看，危险侧和安全侧的故障率都应尽可能的小，在此前提下，达到小的危险比和非对称错误率。换言之，信号设备的故障安全性是建立在设备的高可靠性基础之上的。

4. 安全系统必须有概率的安全目标，并对安全系统进行概率的安全评价。总之，要对安全系统的安全程度做出概率的量化。

二、故障安全概念的单义化及其广义性

传统的铁路信号设备是建立在狭义故障安全概念的基础之上，它单义地规定：设备故障时

倒向"功能停止"侧。这在以信号继电器为主的传统铁路信号设备中是容易实现的。但是，这种故障安全停机的故障安全概念，实际上将降低信号设备的利用率，并且造成列车运行的延误，甚至可能发生危险。况且故障的恢复是通过人的介入来完成的，在要求尽可能小的故障恢复时间内，人的操作难免有误，反而加大故障恢复时间，并有诱发重大事故的可能。此外，在某些领域，如飞行的飞机，是不能把它的安全侧定为"功能停止"的，而必须定为"维持功能"以便"继续飞行"直至降落才能确保安全。又如石油化学设备中对阀门的控制，更不能简单地确定安全侧。这就是说，各个领域的安全侧状态是根据系统的使命而有所不同。总之，故障安全概念应具有明确的广义性。

现在，我们对由于设备故障引起事故的情况作进一步的分析。事故可以用下面的逻辑结构来描述：

$$「事故」=「故障」\wedge「危险侧」 \tag{1-4}$$

如果把「」内的真取值为1，伪取值为0的二值逻辑变量，则可以把(1—4)式的否定认为具有安全的含义。根据迪·摩根法则下式成立

$$「没有事故」=「没有故障」\vee「安全侧」 \tag{1-5}$$

根据(1—5)式安全性可以表达成如下形式：

$$「安全性」=「高可靠性」\vee「故障安全性」 \tag{1-6}$$

(1—6)式的含义是：综合运用避错和容错技术努力提高设备的可靠性，它是实现设备安全性的基础。但是，由于可靠度不可能为1，所以又要求设备具有高的故障安全性。

(1—6)式还告诉我们，应在更加广阔的视野上对待设备发生的故障，使故障安全概念具有更广泛的含义：

1. 虽然设备发生故障，但作为设备的整体仍能正确地完成其功能，这是故障屏蔽；

2. 设备的一部分发生故障，但作为设备的整体仍能正确地完成最低要求的功能，这是故障弱化；

3. 设备发生故障，使设备倒向功能停止，这是故障停机。

由于大规模和超大规模集成电路的价格低廉、小型、省电和较高的可靠性，用容错技术把它组成具有这种广义性故障安全概念的铁路信号设备已经成为现实。

三、故障安全概念的全防护性

所谓全防护性是指，不仅要考虑设备自身的故障而且还要考虑人为差错，两者都不会造成灾害性的结果。多数铁路信号设备，诸如车站联锁设备和区间闭塞设备等，归根到底就是用来防护人为差错造成的危害。但传统的故障安全概念却未把人作为系统的组成部分去研究，因此，所提出的防护措施必然有很大的局限性。

从人—机系统学的观点来看，铁道运输业就是人和机械、人和人组合而成的有机的运营体，它就是一个大型复杂的人—机系统，在这个系统中，人扮演着重要的角色。人的作用由于存在人为差错而有所逊色。因为人总有一些错误地执行规定任务的概率，势必会对系统的可靠性和安全性产生影响。根据 Meister 的研究，人为差错占所有设备故障的20%～50%。根据日本国铁1985年运转事故统计，列车事故的52%是因工作人员的人为错误所引起的。这就告诉我们，故障安全技术不仅考虑设备自身的故障，还必须从"人机工程学"的角度研究人的差错规律，并提出相应的防护措施。

总之，近代故障安全概念具有概率性、广义性和全防护性，它是建立在可靠性理论、容错技术、微电子技术和人机工程学的基础之上的。它对故障安全技术的发展将起着有力地推动作

用。下面我们摘录一下有关故障安全的国际标准，作为本节的结语。

在国际铁路联盟 UIC—738 规程 2.1 款中，对故障安全原则作了明确规定，指出"故障安全原则是这样一种技术，即在考虑了规定的基本条件下(故障假设)，检测出系统故障以很高的概率防止该系统的错误输出，这种检测出的故障要导致信号设备发出限制性信息，也就是导致限制性功能。"

UIC—738 规程 2.2 款指出："具有故障安全功能的铁路信号设备，也不可能达到百分之百的排除任何危险的绝对安全。"

UIC—738 规程 2.4 和 2.5 款中指出："故障检测机制有可能检测不出某些认为不可能出现但又实际会发生的故障。出现这种故障时，便不可能排除危险状态。而且，如果追求过高的安全度时，要受经济方面的制约。"

以上这些规定是值得我们借鉴的。

1.2.2 铁路信号故障安全技术的发展

铁路信号故障安全技术是随着铁路运输的发展和各个时代的科学技术水平为背景不断前进的。回顾这个发展历程，从中总结经验，得到有益的启发，以推动铁路信号故障安全技术的发展。

一、故障安全技术的产生

在设备发生故障时，使其倒向安全侧的故障安全概念早就萌发了。早在 1825 年，世界上出现了第一条铁路——英国的新斯托克顿-达林顿(Newstockton-Darlington)铁路。当时，在夜间是用车站窗口的蜡烛烛光指挥行车的。约定以烛光亮作为停车信号，以烛光灭作为允许信号。这样，常因大风吹灭表示"停止"的蜡烛而发生多次冒进停车地点的行车事故。于是将其含义反过来，把蜡烛亮定为"进行"，蜡烛灭定为"停止"。这就是在初期阶段萌发的故障安全的原始概念。

二、故障安全的设备化

此后，随着科学技术的发展，铁路信号率先完成故障安全的设备化。其中产生过重大影响的有以下几种设备。

1. 臂板信号机。1841 年格列高里(C. H Gregory)发明了易于被司机辨认的臂板信号机。它模仿人们举起手臂发出信号的动作，约定以举起臂板作为停车信号。但由于牵引臂板动作的导线出现折断事故而不能发出停车信号，从而使伤亡事故仍难避免。以此为契机，研制出利用重力显示停车信号的信号机，一直传到今天。机械臂板信号机的结构示意图如图 1—1 所示。它是根据臂板的角度表示信号状态，水平时定为安全侧的停止信号，其具体的故障安全措施是：臂板是木质的，夜间显示用的镜框是铁质的，其重量超过臂板，以回转轴为中心产生反向力矩，保持臂板的水平位置。牵引拐肘的重锤以其自身重量保持下锤状态，此时通过拉杆对显示镜框产生下拉的力，维持臂板的水平位置。这样一来，一旦拉杆折断或导线折断，依靠镜框和重锤的重力，使臂板成为水平，倒向安全侧。这种重力法原理后来成为故障安全技术的重要方法之一。

2. 机械联锁设备。1856 年 John Saxby 提出并在英国 Bricklayer Arms 联络站上装设了机械联锁设备。随后由 Farmer 对此加以改进，所以称为 Saxby—Farmer 式联锁装置。联锁往往是双方相互制约的先后顺序关系。例如当道岔位置不对、禁止信号机显示允许信号；信号机一旦显示允许信号后，又将道岔锁闭，不准许它再变位。用机械的方法实现了信号机和道岔之间的这种联锁，防止操作人员的错误办理。

3. 信号用继电器。1870 年左右，具有非对称错误特性的信号用继电器就开始使用了。这种继电器是把无电闭合的接点组规定为安全侧，有电闭合的接点组规定为危险侧。当发生断电、断线故障时，必须使反映危险状态的前接点组自动断开，反映安全侧状态的后接点组自动闭合。这种继电器的结构示于图 1—2，实现故障安全的技术措施是：

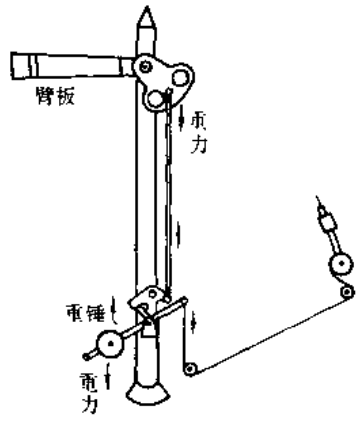

图 1—1 机械臂板信号机结构示意

(1)有电闭合的接点组采用银和炭的接点，银和炭成为一个不可熔性的组合，使其不能因电弧、火花或大电流造成熔接而保持吸起位置。

(2)衔铁的装配是依靠它的重力而不用弹簧力，在失去电能的时候，使有电闭合的接点断开。

(3)动接点组与衔铁间采用硬性连接，以保证衔铁和接点动作的一致。

(4)磁路空气隙是经过仔细选定的，并由非磁性的安全止钉保持这一空气隙。

(5)继电器端子柱之间的空隙，其漏电和耐压的大小一定要足以使得闪电和其它高压脉冲不会损坏面板和将其绝缘电阻减至不安全的程度。

这样结构的结果，当电路、线圈发生故障时，后接点组闭合的概率大大超过前接点组闭合的概率，使其具有非对称错误特性。如用后接点组构成红灯显示，前接点组构成绿点显示，当发生故障时，以较高的概率变成红灯显示，从而实现故障安全原则。

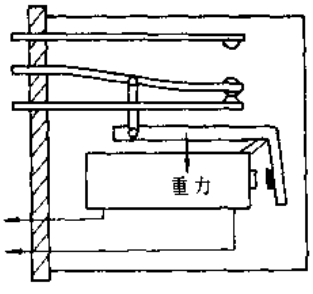

图 1—2 信号用继电器

4. 轨道电路。1872 年美国的维·鲁滨逊(V. Robinson)发明了轨道电路。最初是开路式轨道电路。列车进入轨道电路区段，由于钢轨断裂、连接线断线，继电器不能励磁吸起，发生了不能显示停止信号的事故。因而，三年后产生直流闭路式轨道电路，如图 1—3 所示。在没有列车或车辆时，钢轨上流通电流，使轨道继电器励磁吸起闭合前接点组。当列车或车辆占用轨道电路、或连接线断线、或钢轨裂缝时，轨道继电器会失电落下闭合后接点组，表示区段占用，显示停止信号，实现故障安全。这里的安全侧与轨道电路的开路或短路状态相对应。

5. 继电联锁设备。1929 年 Chicago. Rockisland 和 Pacific 铁道，在美国 Illinois 州的 Blue Island 设置第一个继电联锁装置。它是用信号继电器，根据闭路原理和安全对应法则组成实现信号机、道岔、轨道电路电气联锁的继电器电路。

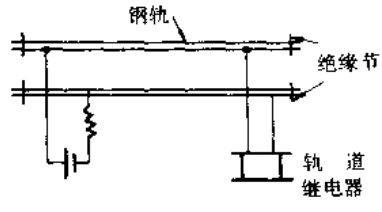

图 1—3 闭路式轨道电路

在这个阶段，铁路信号仍停留在狭义的故障安全概念上。故障安全技术主要以实际经验为基础，吸收各个时代的先进技术而发展起来。从机械的、电气的到电子的信号设备，设计使用了许多故障安全技术。特别是经过实际使用而改进了的安全技术，成为今天以故障安全为中心内容的铁路信号安全技术的重要内容。这当中，集中了前辈们的智慧及丰富的经验，这对后来的铁路信号设备的设计是不可缺少的珍贵资料。

但必须指出，这个时期的铁路信号故障安全技术有两个严重的缺陷：

1. 缺乏理论性，对大量的通过实践积累起来的资料，没有上升为故障安全逻辑理论。对叫做时序机宝库的继电联锁，几乎没有进行理论性的研究。在1955年，日本的持田喜一部先生进行了用布尔代数表现继电联锁逻辑的研究，但因中途逝去而终止。

2. 缺乏系统性。对大量的实践积累起来的资料，没有进行整理形成一个完整的体系。

三、故障安全逻辑理论的问世和发展

面对半导体技术的发展，铁路信号设备的微电子化提到了日程上来。在这样的背景下，故障安全逻辑理论的研究，首先在日本，从1963年到1965年的三年间由信号保安协会进行的研究为开端而盛行起来，所进行的研究是以"电子技术信号设备的研究"为主体展开的，最后提出了相应的报告。它成了进行故障安全逻辑研究的重要文献。

1965年以来，日本学者渡边昭治等首先提出了二值故障安全逻辑系统的理论，其中包括考虑冗余手段的故障安全问题。他们虽然接收了传统的故障安全概念，但它们的研究却具有如下特点：以现代半导体电子技术为基础，以离散结构、数理逻辑以及概率论等为理论工具，以研究高速系统的故障对策为目标。因此，它与前面所述的具体设备的故障安全技术不同，他们探索的是一般故障安全系统的构成规律。可以说，他们的研究成果为故障安全逻辑理论打下了基础，使铁路信号故障安全技术进入了一个新阶段。

起源于传统故障安全的二值故障安全逻辑系统，由于在某些系统中逻辑0和逻辑1之间并不确定地存在着一方比另一方更为安全的意义，所以日本的学者们又提出了三值故障安全逻辑系统和广义的多值故障安全逻辑系统，以及交替故障安全逻辑系统。

前述的故障安全逻辑都需要非对称错误特性元件，而实现这种特性的元件往往是很困难的。于是人们试图用具有对称错误特性的集成电路芯片实现故障安全逻辑。这方面的研究后来由自校验逻辑理论所继承。1968年IBM公司的W. C. Carter第一个提出了自校验的基本概念，1973年D. A. Anderson等给出了自校验逻辑的定义，1979年M. Dinz等发表了"自校验和故障安全组合电路、时序电路的统一设计"的论文，将自校验和故障安全两个概念建立了密切地联系，给出了统一的设计方案。这些研究成果，对以后的故障安全逻辑的研究工作产生了很大的影响。

四、故障安全技术的系统化

为了继承和发展铁路信号经验性故障安全技术，有必要从工程学的角度进行总结，作体系化的整理。

在日本，从1975年起东京大学宇都宫教授为委员长的国铁部外委托研究委员会进行了研究，于1978年汇编成"信号安全技术调查书"。后来，奥村绫正等人于1981年3月提出了"系统安全工程学的现状和铁路信号引人"的研究报告，对前一报告进一步加以完善。报告中对铁路信号安全技术进行分类，使之体系化，具体内容概况如下：

故障安全；

危险侧故障的减低；

防错办；

故障弱化；

多重系化；

后备；

故障诊断、恢复；

安全余裕。