信息技术丛书

数字系统的故障诊断与可靠性设计

（第二版）

杨士元　编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书主要介绍以下三部分内容:数字系统测试和故障诊断技术的理论和技术,其中重点介绍了测试向量的生成技术和方法以及测试向量的优化技术;数字系统可测性设计的基本概念和相关技术,其中对边界扫描设计的原理和有关标准 IEEE 1149.1 作了较详细的叙述;数字系统的可靠性设计,包括数字可靠性的基本概念、硬件容错技术、全自检技术、编码纠错技术和软件容错技术等。此外,书中附有习题和答案或提示。

本书是自动化和计算机专业的本科生和研究生教材,也适合于从事数字系统设计、测试和维护的技术人员作参考书。

书　名:数字系统的故障诊断与可靠性设计(第二版)
作　者:杨士元
出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http:// www.tup.tsinghua.edu.cn
印刷者:北京市人民文学印刷厂
发行者:新华书店总店北京发行所
开　本:787×1092 1/16　印张:22.25　字数:521 千字
版　次:2000 年 4 月第 2 版　2000 年 12 月第 2 次印刷
书　号:ISBN 7-302-01136-2/TP・334
印　数:4001～9000
定　价:25.00 元

《信息技术丛书》

出 版 说 明

人们称当今的时代为信息时代。信息科学技术的快速发展和广泛渗透已经成为现今社会的一个重要的时代特征。人类社会的生产活动和生活质量，比以往任何时代，都更加得益和依赖于信息技术的成就和发展。自动化是信息技术领域的主要组成部分之一，包括信号和信息处理、模式识别、知识工程、控制理论、自动化技术、传感技术、自动化仪表、系统工程、机器人控制、计算机控制与应用、网络技术等在内，都和信息科学与技术有着直接和密切的关系，几乎涉及到了信息的检测、分析、处理、控制和应用等所有的方面。正是基于当今时代特点和科技发展态势这个大视野，结合自动化类专业人才培养模式及教学内容体系的改革，我们规划和组织了这套丛书的编写和出版。这套丛书的读者，定位为自动控制、过程自动化、计算机、电子工程、电气工程、动力工程和机械自动化等系科的高年级大学生和研究生，以及工作于这些领域和部门的科学工作者和工程技术人员。

十年前，我们曾经组编和出版过一套《信息、控制与系统》系列教材，产生了比较大的社会影响，其中的许多著作至今仍然为国内很多高等学校用作教材，并为广大相关的科技人员作为进修和自学读物。现在组编和出版的这套《信息技术丛书》，从一定意义上可以说，就是先前的那套系列教材的发展和延伸，以反映新的进展和适应新的需求，匹配于变化了的时代和发展了的科技。列入这套丛书中的著作，大多是清华大学自动化系等开设的课程中经过较长教学实践而形成的，既有在多年教学经验基础上新编的教材，也有原系列教材中的部分教材的修订版本。总体上，这套丛书仍将保持原系列教材的求新与求实的风格，力求反映所属学科的基本理论和新近进展，力求做到科学性和教学性的统一，力求体现清华大学近年来在相应学科和领域中科学研究与教学改革的成果。

我们希望这套丛书，既能为在校大学生和研究生的学习提供内容较新和论述较为系统的教材，也能为广大科技人员的继续学习与知识更新提供适合的和有价值的参考书。我们同时热忱欢迎，选用这套丛书的老师、学生和科技工作者指出批评和建议。

《信息技术丛书》编委会

1999 年 10 月

《信息技术丛书》编委会

第二版前言

本书自1989年出版以来已经过去十个年头了。在这十年之中，微电子技术发展非常快。作为一本专业性的教材，尤其是关于数字电路测试技术的教材，有些内容已显得陈旧和落后，而一些新技术又没有纳入，不利于学生和读者了解国内外在该领域的发展动向。而在国内不少研究单位和高校，尤其是军事部门的一些单位，对数字系统的测试有越来越急迫的需求。基于上述二点，决定对该书作较大幅度的修改和增删，作为该书的第二版与读者见面。

在这次修订的过程中，鉴于目前时序电路的可测性技术日臻完善和成熟，其测试常在内驻自测试中完成，因此对相关内容作了较大的删改。但为使本书较为系统化，同时考虑到国内在可测性设计领域尚属起步阶段，现有的系统和设备大多还没有使用或采纳，因此仍保留了一些基本方法的介绍。第二版中增加的篇幅主要集中在第5章和第6章，即关于数字系统的可测性设计和数字系统的可靠性设计两个部分。前者在国际上发展很快，目前已有了国际上的标准，并被一些大公司广泛采用，在国内也引起了相当的重视，因此在第5章中增加了目前可测性设计的主要技术——边界扫描设计以及相应的国际标准IEEE 1149.1，以便读者掌握它的基本原理和该方面的发展动向。在数字系统的可靠性设计方面增加了复杂系统的可靠性分析的内容，以便读者掌握更多的分析方法和技术，以适应当前系统越来越复杂的状况。

在这十年之中，在数字系统的测试和可靠性设计领域中，涌现的新理论和新方法是很多的。但考虑到教材主要是介绍基本原理和方法，同时考虑到教学学时的限制（清华大学自动化系的研究生学位课程讲授约为30学时），还考虑到本书的连贯性和系统性，因此不可能再增加更多的新内容，这也是一件遗憾的事。

在本书第一版出版之后，作者收到了不少读者的来信，给予作者很大的鼓励。有的读者对本书提出了宝贵的意见，指出了书中的一些不当之处，在对本书作修订之际，作者对这些读者表示衷心的感谢，并希望读者继续关注本书，不吝赐教。在这次修订时，虽然已仔细纠正那些不当之处，但仍难免有不妥和错误之处，恳请读者批评指正。

作　者

1999年12月于清华大学自动化系

第一版前言

随着数字计算机日益广泛的应用，数字系统的可靠性越来越显得重要。作为提高数字系统可靠性的两个主要途径的故障诊断和可靠性设计经过近三十年的发展，在理论上已日趋完善，并出现了各种具有实用价值的算法和程序。近年来，由于超大规模电路的出现，以及由此导致的数字系统复杂性急剧提高，使常规的故障诊断技术和可靠性设计变得十分复杂和困难，因此随之而兴起的可测性设计已成为当前一个非常活跃的研究领域。

本书主要叙述数字系统故障诊断、可测性设计和可靠性设计的基本概念和主要方法，并力求反映出近年来的最新技术和研究成果。它是自动化仪表与装置等专业高年级学生和研究生用教材，也可作为其他有关专业的研究生或本科生的选修教材。为适应各种不同的教学要求，书中内容可分成两个层次，其中一个层次着重于阐述基本概念和基本方法，在目录中以“*”标出，讲授这部分内容约需 20 学时。另一个层次基本上包括全书的主要部分，讲授时间约需 40～50 学时，为便于从事该领域研究工作的科技人员自学，除了引入比较多的例题外，还附有习题和绝大部分习题的答案或提示。此外对重要的结论均注有原始文献，以便读者查阅。

全书承童诗白教授审阅，并提出许多宝贵的修改意见，在此表示衷心感谢。

由于作者水平所限，书中难免有不妥和错误之处，恳请读者批评指正。

作　者

1989 年 2 月于清华大学自动化系

目　　录

第1章 绪 论

1.1 数字系统测试的发展概况

数字系统故障诊断技术的发展[1.1~1.4]，是同数字系统中的元件、结构和应用，尤其是数字计算机的发展紧密联系的。由于数字系统已经广泛应用于各行各业，为保证其可靠运行，故障的诊断是一个必不可少的重要环节。

无论是元件还是电路和系统，由于制造工艺的限制、使用寿命以及工作条件等影响，故障的产生是不可避免的。处理故障有两种基本的策略，均可用硬件和软件结合起来实现。第一种策略是采用冗余技术，将故障的影响掩盖起来。这种策略主要用于高可靠性的，而且在一段时间内既要保证连续运行，但又无法修理的地方，比如航天航空等一些要害部门。但是随着故障的增多，最后故障的影响总不能全部掩盖起来。另一种策略是及时诊断，及时修理，这虽然经常需要停止系统的工作，甚至还要脱离整个系统，对用户不甚方便，但在大多数情况下还是必要的，而且也是可能的。

故障诊断与故障掩盖往往是矛盾的，因为可掩盖(冗余)的故障经常是不可诊断的。现在已经提出了一种巧妙的冗余技术，使得系统在运行时是故障冗余的，即可掩盖故障。而在测试或修理系统时，故障又是可诊断的，即此时不再掩盖故障。这样就比较好地解决了系统短期的极端可靠性要求和后期故障检测和诊断之间的矛盾。

早期的数字系统故障诊断是依靠工程技术人员凭借自己的丰富经验和理论知识，并借助一些常规的工具(如万用表、示波器等)来完成的。这不仅对技术人员的素质有很高的要求，而且故障诊断的速度慢，质量差。尤其是系统日趋复杂，这个矛盾就更加突出，这就迫使人们研究新的方法和技术来完成这项工作，而计算机的迅速发展，尤其是微型计算机的普及，为故障检测和诊断提供了物质基础，使测试与诊断的自动化成为可能。

故障自动测试与诊断的基本思想是暗箱理论，即被测对象是一个“神秘”的不可及“暗箱”，在不允许打开“暗箱”但又要了解“暗箱”的情况下，只有施加一系列的激励，再根据相应的输出响应去分析和“猜测”“暗箱”中的“奥秘”。其工作框图如图 1.1.1 所示，其中测试器要完成四项工作：

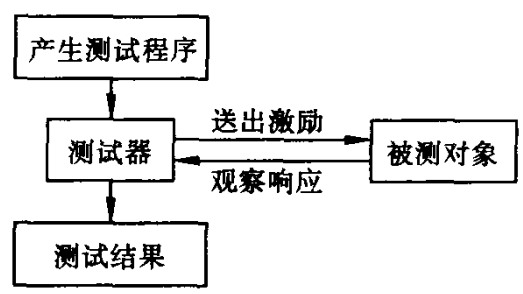

图 1.1.1 系统故障诊断的工作框图

① 向被测对象送出测试的激励信号(测试矢量)；

② 接收被测对象在相应激励下的响应信息；

③ 根据激励与响应之间的关系分析并“决策”下一个激励矢量；

④ 根据激励序列和响应序列来确定故障的类型和地点。

从故障诊断的工作框图可以看出，它与系统的计算机辅助设计(CAD)有相似之处，它们都需要施加实际的激励并接收响应，而且要“猜测”系统中的参数。两者的不同之处是：在故障诊断和测试中，一般都已知道了系统的拓扑结构，它要“猜测”的内容只是元件或部件的参数，因此它的解有时是唯一的，即它的随意性不是很大。而在系统综合中，它要“猜测”系统的拓扑结构和元件或部件的参数，因此它的解很少是唯一的，即它的随意性比较大。正因为故障诊断与系统综合在本质上有很大的差异，因此在研究方法上也有极大的差异，所以，诊断理论在系统和网络理论中已独自成为一个重要的领域，而不是附属于已有的某个领域。

故障诊断理论与系统的辨识理论在很大程度上有相似之处，因此在故障诊断中也常采用系统辨识的方法。但是由于诊断问题是已知系统的结构来估计参数，而不必猜测系统的结构，因此两者在研究的方法和形成的理论方面都有相当的差异。例如，关于元件或部件的参数容差问题，在系统辨识问题中不是一个非常突出的问题，而在诊断中却是一个必须解决的问题。又如在诊断中，元件参数的变化或元件的损坏，必须以元件的结果来体现，而在系统辨识中经常可以用结构的结果来体现，一般说来，系统辨识是相对正常系统而言的，而诊断是在已知正常系统的前提下，相对故障系统而言的。

在系统故障诊断中，核心的问题是确定施加什么样的激励，可以使故障激活(即使故障能够反映出来)，同时能在可及端测量出来。因此还要确定在什么地方施加激励，在什么地方进行测量。

最初的故障诊断系统主要用于作功能测试，而且使用了特殊的硬件设备。如 1953 年 Eckert 所采用的 BINCA 计算机就是用两个相同的处理器同步进行工作，并随时进行比较，视其是否有相同的计算结果来判断是否有故障，维修人员可根据两个处理器的不同状态来确诊故障的位置。同年 Dagget 和 Rich 在 Whirl-Wind 机上采用了循环程序控制技术，使得技术人员可以通过控制启停开关来重复执行预选的程序，并在一些主要的检验点观察响应，以诊断系统内的故障。随着系统的增大和复杂化，专用仪器及硬件设备逐渐成为辅助手段，而主要依靠故障诊断软件。故障诊断软件也只能检查系统的功能，而不是系统的硬件设备。其主要做法是令系统作一些复杂的运算或执行一些复杂的逻辑操作，根据操作的结果是否正确来判断系统的功能是否正常。但是，依靠这些方法不可能在有限的时间内，对一个复杂系统作全面而完整的测试，同时，可诊断的范围也总有局限性，有些“死角”的故障不易诊断出来，因此改进的方向是要检查系统的硬件设备。

检查硬件设备的研究工作是从最简单的组合逻辑电路开始的。Eldred 在 1959 年提出了第一篇关于组合电路的测试报告。尽管它只是针对单级或两级组合电路中的固定型故障作检测，但它已实际应用于第一代的电子管计算机 Datamatic-1000 的诊断中，并揭开了数字系统故障诊断的序幕。Eldred 指出，一个三输入端的或门，它在输入端的故障可以用输入矢量(100)，(010)和(001)来测试，其中每个测试矢量还可检测输出端的 s-a-0(stuck-at-0)故障。为了检测输出端的 s-a-1(stuck-at-1)故障，还需要增加输入矢量(0 0 0)。

Eldred 提出的方法只能解决两级以内的组合电路的故障测试问题。D. B. Armstrong

在 1966 年根据 Eldred 的基本思想提出了一维通路敏化的方法，其主要思路是对多级门电路寻找一条从故障点到可及输出端的敏化通路，使在可及端可以观察到故障信号。利用这种方法，确实解决了相当多的组合电路的故障诊断问题。当时人们认为，非冗余的组合电路中任一故障信号都是沿某一条通路传输到可及端的。直至 1976 年，Schneider 提出了一个反例(见图 1.1.2)，证明了某些故障信号只通过一条通路是不可能传输至可及输出端的，而必须同时沿两条或两条以上的通路传输，才能在可及输出端测到故障信号。

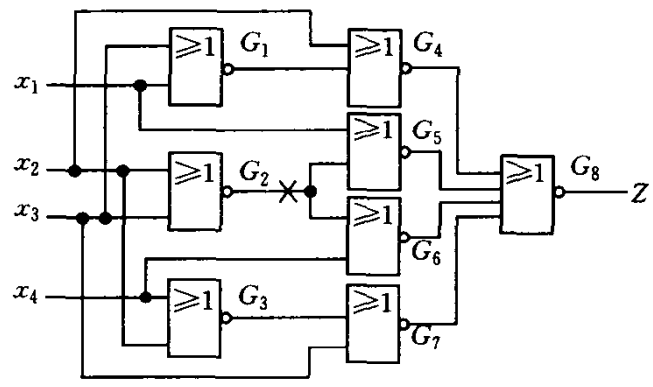

图 1.1.2　Schneider 反例电路

Schneider 在其举出的反例中指出：或非门 G_2 输出端故障 G_2(s-a-0)只沿 G_2—G_5—G_8 或 G_2—G_6—G_8 中的任意一条通路作传输是无法在可及输出端 Z 得到故障信号的。因为敏化通路 G_2—G_5—G_8 的必要条件是 $G_4=G_6=G_7=0$，由 $G_6=0$，则唯一条件是 $x_4=1$；再由 $x_4=1$ 和 $G_7=0$，可得唯一条件 $x_3=1$。但是为了检测故障 G_2(s-a-0)，敏化这个故障的唯一条件是 $x_2=x_3=0$。因此，出现了对输入 x_3 的矛盾要求。换句话说，如果要使故障 G_2(s-a-0)沿 G_2—G_5—G_8 传输，则故障 G_2(s-a-0)是反映不出来的；如果要使故障 G_2(s-a-0)激活，则这条单一的通路是无法敏化的。根据电路的对称性可知，故障 G_2(s-a-0)只沿通路 G_2—G_6—G_8 也是不可测的。可是事实上，这个故障在输入($x_1\ x_2\ x_3\ x_4$)=(0 0 0 0)时是可测的，分析其原因是，这个故障信号是同时沿上述两条通路向可及输出端 Z 传输的。

Schneider 指出了一维通路敏化存在的问题，但是没有提出解决这个问题的方法。事实上罗思(Roth)于 1966 年提出的著名的 D 算法就已经考虑了故障信号向可及端传输的所有可能的通路(包括多通路传输)。经实践证明，这种方法是可行的。以后罗思从理论上证明了 D 算法的确实性，因此 D 算法一直沿用至今。虽然以后对此有不少改进，但都没有超出罗思的基本思想。因此，从理论上说，组合电路故障检测和诊断在罗思的 D 算法中已到达了最高点，在实际应用中，脱胎于 D 算法的 PODEM 算法和 FAN 算法已经臻于完善，到达了完全实用的阶段。在罗思之后，Seller 等提出的布尔差分法与 Thayse 提出的布尔微分法，虽然在实际使用中存在一定的困难，但是使通路敏化的理论得到了系统化，因此这两者在数字系统诊断理论中均占有重要的地位，是进行理论研究的必要工具和基础。

罗思的 D 算法从理论上解决了组合逻辑电路的测试问题，即任何一个非冗余的组合逻辑电路中任意单故障都可以用 D 算法来找到测试它的测试矢量。但是在实际使用中还存在着计算工作量十分浩大，以至对大型电路很难付诸实施的问题。虽然各种改进方法在不同程度上提高了运算速度，但总的计算工作量还是很大的。Armstrong 在 1966 年提出

了 enf(等效正则)法,其核心问题是寻找一个可诊断(检测)电路内全部故障的最小测试集。波格(Poage)和博森(Bossen)等提出了用因果函数来找诊断所有单故障和多故障的最小检测集,并在小型的组合逻辑电路测试中取得了比较满意的结果。但是上述几种方法通常都要处理大量文字型的数据,所需的工作量和计算机内存容量都比较大,因此对大型的组合电路难以付诸实用。我国学者魏道政教授等提出的多扇出分支计算的主通路敏化法以及较为直观的图论法,在实际应用中显示出较大的优越性[1·6]。

随着系统和电路规模的增大和元件集成度的提高,大型组合电路故障检测和诊断日趋迫切,对计算机的运算速度要求也越来越高,所需的计算机内存容量也越来越大,使得某些算法已失去了实用的价值,因此必须研究和探讨新的方法,或探索某一类系统或部件的专用测试方法,这也就是为什么数字系统故障理论和方法的研究始终没有停止的原因之一。比如,随着 PLA(programmable logic arrays,可编程逻辑阵列)的出现和广泛应用,PLA 的特殊测试理论和方法纷纷出现。有趣的是,过去认为没有实用意义的穷举测试方法,随着电路规模的增大而有了新的发展。因为穷举测试的测试矢量的产生是非常简单的,1984 年 Archambeau 等提出的伪穷举法,为穷举法用以解决大型组合电路的测试开拓了新的途径。

时序电路的测试比组合逻辑电路的测试要困难得多,其主要原因有三个:一个原因是在时序电路中存在着反馈线,而对反馈线的处理是比较困难的,它不仅对故障的检测和诊断带来不便,而且使电路的仿真也甚为困难;第二个原因是由于存在着存储元件,因此电路中存在着状态变量的初态问题,在没有总清或复位的条件下,这些状态变量的初态是随机的,要寻找一个复位序列使这些状态变量转移至已知的确定状态,并不是一件轻而易举的事情,尤其是当电路存在着一些故障时,这种复位序列是否存在还是一个问题;第三个原因是时序元件,尤其是异步时序元件,对竞态现象是异常敏感的,因此产生的测试序列,不仅在逻辑功能上要满足测试要求,而且要考虑到竞态对测试过程的影响。正因为时序电路的测试存在着上述三个难以解决的问题,因此它的测试理论和方法的研究进展一直比较缓慢,切实行之有效的方法也比较少。

解决时序电路测试问题的最初途径是沿用组合电路的算法,但由于要对电路的状态作估算,因此使计算工作量陡增。Hennie 在 1964 年首先提出了把时序电路"复原"的输入序列的问题,但实际上并非所有的时序电路都存在这样的"复原"序列。

为了较好地解决时序电路的测试问题,相继提出了逻辑函数的多值模拟法,其中比较成功的有三值、六值和九值布尔模拟。多值布尔模拟中所引入的新的布尔变量,主要是为了解决时序系统中状态变量的初值设置,以及在测试过程中某些元件的未知状态或随意状态的表达问题。这些多值的布尔模拟方法不仅使时序电路的测试理论日趋完善,而且使时序电路的测试成为可能。目前常见的方法有九值算法、线路-时间方程算法和 M0M1 算法等。我国学者提出的 H 算法[1·7]也作了有益的尝试,并取得了一定的成果。

在研究面向故障的测试矢量产生方法的同时,时序电路功能测试问题也得到了广泛的重视。这种测试方法不考虑电路的结构,而只考虑电路或系统的功能流程,它只检验系统的逻辑功能是否正确,而不考虑故障的定位问题,因此它不能替代一般的测试问题,但在验证一个设计方案和检验生产厂家的产品时是非常有用的。

不管是时序系统，还是组合逻辑系统，虽然至今都已有了一些成熟的理论和实用方法来测试，但是它们的计算工作量和测试的开销都是很大的。尤其是现在系统的规模越来越大，测试的矛盾也日益尖锐。人们开始认识到，传统的系统设计过程，即设计人员主要考虑完成一定的逻辑功能的系统设计，测试人员根据已有的系统或器件来研究测试方法和开发测试设备，已经越来越不适应生产的实际需要。由于测试的开销在系统设计中占有的比例急剧增长，已经不能再把测试问题看作是一个附属的次要问题，而应看作系统设计中的一个重要的组成部分。例如，据美国有关公司统计，当今一些 PCB(printed circuits board 印刷电路板)的测试开销已占整个生产过程中总开销的 50%以上，因此单纯研究新的测试方法和开发新的测试设备已很难满足厂家生产的需要。所以，根本的解决方法是在进行系统设计时就充分考虑到测试的要求，即要用故障诊断的理论去指导系统设计，这就是所谓的可测性设计。

从故障诊断理论角度看，系统中各节点的值越易控制(容易使故障得到激活)，故障信号越易观察或测量(容易使故障信号传输至可及端)，则系统中的故障越易检测和诊断(定位)。因此，可测性设计中首先要解决可测性的度量问题，使可测性有一个量化的依据。至今已有多种可测性的度量方法，例如 Stephenson 和 Goldstein 各自提出了不同的度量方法，但在不同程度上还存在着局限性，在可测性的描述上都比较粗糙，所以研究新的、更符合系统可测性特性的度量方法仍是一个重要课题。

可测性设计要研究的主要问题是：什么样的结构容易作故障诊断；什么样的系统，测试时所用的测试矢量既数量少，产生起来又比较方便；测试点和激励点设置在什么地方，设置多少，才使得测试比较方便而开销又比较少等。

到目前为止，可测性设计方兴未艾，是一些学者的重要研究课题。现在已有了一些比较成功的可测性设计方法。其中最突出的是边界扫描设计技术的发展和 IEEE 1149.1 标准的制定，使系统的可测性设计理论和方法的研究到达了一个新的高度，并已具有了实用的价值。相对而言，时序电路的可测性设计进展更快一些，例如，适用于时序电路的扫描设计就是一种比较典型的方法。虽然扫描设计要增加许多硬件的开销，但由于它较好地解决了时序电路的测试问题，同时由于现在元件制造工艺的迅速发展，为扫描设计提供了物质上的基础，因此得到了广泛的应用。它不仅应用于系统、模块和 PCB 中，也已经应用于大规模集成芯片中，使得它们能得以自检。这不仅使系统或部件的故障诊断得以简化，也大大提高了系统的可靠性。值得指出的是：正因为时序电路的可测性设计进展比较快，所以时序电路的测试研究相对比较少了，而组合电路的可测性设计解决得不甚理想，因此大型电路的测试问题仍是研究的重要课题。可见这两者是相辅相成的。

在组合电路中，PLA 由于它结构上的规整性，因此它的可测性解决得比较好，到目前为止，已有比较理想的设计方案[1.8]，虽然它还存在着测试故障率没有达到百分之百，测试速度较低，附加电路对 PLA 的运行速度有一定影响等问题，但由于增加的硬件比较少，测试矢量数少，且测试矢量比较规整，因此已经有了实用的价值。

系统进行故障检测和诊断的最终目的是使系统能长期可靠运行。由于计算机的广泛使用，系统的规模越来越大，可靠性的问题也越来越引起人们的重视。可以这么认为，没有可靠性，就没有自动化。

提高可靠性的基本思想有两条：一是增加“多余”的器件或子系统来“掩盖”故障，即采用容错技术；二是加强系统的自检功能，使系统始终以完好的状态来进行工作。最初的容错技术是从两支并联的二极管代替一支二极管可以容错一支二极管的开路故障而提高可靠性的事实得到启发，发展成四倍冗余线路；从多数表决的结果具有较高的可靠性这一事实研究出了三模冗余结构；此外，吸收了通信理论中纠错码的方法，提高了系统中信息传输、存储以及运算中的可靠性。为了提高系统或部件长期运行的可靠性，又研究了系统自检的方法以及自检自修的系统。同时利用系统硬件和软件的相互作用，使系统能自动检测出故障，并自动恢复功能，从而进一步提高了系统的可靠性。可靠性设计至今在国际上仍是一个极为活跃的领域，如美国“国际电机和电子工程师学会”(IEEE)自 1971 年起，每年都要召开一次“国际容错计算年会”，并出版论文集，至今已召开过二十多次会议。

容错技术主要要解决冗余模块数量的确定、故障模块的检测与诊断以及故障模块的切换等关键技术。由于采用各种不同的方法来解决上述这三个问题，出现了各种各样的容错设计方案。

最后需要指出的是，人们对计算机硬件的可靠性一直是极为关注的，但是对软件的可靠性问题还没有引起足够的重视，甚至有的人认为，计算机的软件不存在可靠性问题。随着软件规模的增大，它的应用范围逐渐扩大，通过实践逐渐使人们认识到软件可靠性问题的重要性和复杂性。一般说来，软件的可靠性和硬件的可靠性问题是不同的，它的故障主要不是来源于运行过程中的老化或损坏，而是来源于软件的编制过程和各种软件的组合过程。但是由于软件的编制目前仍主要依靠手工编制，各种差错和缺陷很难避免，而现在又没有一种行之有效的检查软件可靠性的理论和方法，导致无法科学地评价一个软件的可靠性。因此，研究计算机自动编程，开发评价计算机软件可靠性的理论和方法，是当前数字系统可靠性研究领域中极需解决的课题。

1.2 故障和故障模型

1. 故障

一个逻辑元件、电路和系统，由于某种原因而导致其不能完成应有的逻辑功能，则称这个元件、电路和系统已经失效(failure)。而故障(fault)是指一个元件、电路和系统的物理缺陷，它可以使这个元件、电路和系统失效，也可能不失效，换句话说，存在有一定故障的元件、电路和系统仍有可能完成其固有的逻辑功能。

故障可以用故障的性质、故障值、故障的限度和范围以及故障的时间间隔等参数来描述。故障性质是指故障是属于逻辑故障还是非逻辑故障。凡是使电路或系统中某一节点的逻辑值为正常值的相反值的故障叫做逻辑故障，如元件输出短路、输入端开路、元件损坏以及竞态故障等均属于逻辑故障。除逻辑故障以外的故障都称为非逻辑故障，如同步时序电路中的时钟故障和电源的失效等。故障值是指电路或系统中故障产生的错误逻辑值是固定的，还是可变化的；如果是固定的，那么它的固定值是多少。故障的限度及范围是指故障的影响是局部型的还是分布型的。局部型故障只影响单变量，而分布型故障则影响多

个变量。例如逻辑故障一般都是局部性的故障，而同步时序电路中的时钟故障是属于分布型的故障。故障的时间间隔是说明故障是永久性的，还是间歇性的。

有的地方还采用硬故障和软故障的概念，这是沿用模拟系统中的故障概念。一般说来，器件参数的变化（如输出电平的偏移、输入短路电流的增大等）叫做软故障，而永久性的损坏故障叫做硬故障。但是在数字系统故障诊断中很少采用这两个概念，因为一般无法诊断出这种软故障的具体情况，往往只能转化成固定型的永久性故障或间歇性故障来研究。

2. 故障模型[1.4][1.5][1.2]

一个元件、电路或系统的物理故障是千变万化的。一方面故障的种类就是各种各样的，就以短路故障为例，一个门电路输入端短路，两个输入端之间的桥接短路，一个门的输入端与输出端之间的短路，奇数级门或偶数级门输入与输出端之间的短路等等，引起的失效结果会有很大的差异。另一方面，故障的数目在各种系统中有很大的差异，而多故障组合的情况就更多了。因此，为了研究故障对电路或系统的影响，诊断（定位）故障的位置，有必要对故障作一些分类，并构造最典型的故障，这个过程叫做故障的模型化。用以代表一类故障（对电路或系统有类似影响的故障）的典型故障称为模型化故障（有的地方也称之为逻辑故障，但这容易同故障性质中的逻辑故障混淆）。

故障模型化的基本原则有两个：一个是模型化故障应能准确地反映某一类故障对电路或系统的影响，即模型化故障除应具有典型性、准确性，还应有全面性。另一个原则是，模型化故障应该尽可能简单，以便作各种运算和处理。显然，这两个原则是矛盾的，因此往往要采取一些折衷的方案。由于解决的问题不同和研究的侧重面不同，而采用的故障模型也不同，因此在决定使用什么样的故障模型时，首先要考虑所研究对象的重点是什么，所研究电路和系统的实现技术和采用器件是什么，最后还应考虑到研究用的设备、软件和其它条件。总而言之，故障的模型化在故障诊断中起着举足轻重的作用，一个好的故障模型化方案往往能使故障诊断的理论和方法得以发展和完善。下面介绍几种目前常用的模型化故障。

（1）固定型故障

固定型故障（stuck faults）模型主要反映电路或系统中某一根信号线（如门的输入线或输出线、连接导线等）上的信号的不可控性，即在系统运行过程中永远固定在某一个值上。在数字系统中，如果该线（或该点）固定在逻辑高电平上，则称之为固定 1 故障（stuck-at-1），简记为 s-a-1；如果信号固定在逻辑低电平上，则称之为固定 0 故障（stuck-at-0），简记为 s-a-0。

固定型故障模型在实际应用中用得最普遍，因为电路中元件的损坏、连线的开路和相当一部分的短路故障都可以用固定型故障模型比较准确地描述出来，而且由于它的描述比较简单，因此处理故障也比较方便。以 TTL 门电路为例，输出管的对地短路故障属于 s-a-0 故障，而输出管的开路故障属于 s-a-1 故障。任何使输出固定为 1 的各种物理故障都属于 s-a-1 故障。

需要着重指出的是，故障模型 s-a-1 和 s-a-0 都是相对于故障对电路的逻辑功能而言