潜通路分析技术①

严殿启

(北京航天自动控制研究所,北京,100854)

摘要 阐述了潜通路的概念并指出了它在复杂系统中造成的巨大危害。简要地介绍了潜通路分析技术在国外的应用与发展。重点介绍一种我国自行开发的通用潜在分析系统(CSAS)。该系统已成功地应用于实际的航天工程之中。

关键词 潜通路,潜在分析技术,功能追踪法。

Sneak Passage Analysis Technology

Yan Dianqi

(Beijing Aerospace Automatic Control Institute, Beijing, 100854)

Abstract The concept of sneak passage is introduced and its serious hazard in complex critical system is pointed out. The application and development of sneak passage analysis technology in other countries of the world are briefly described. Emphasis is laid on presenting a conventional sneak analysis system (CSAS) . This system is developed by our project team and applied to practical aerospace engineering successfully.

Key Words Sneak Passage, Sneak analysis technology, Function searching method.

1 潜通路概念及其危害

潜在电路(Sneak Circuit)的概念是最早由美国波音公司在完成阿波罗登月计划期间针对电子电气系统提出来的。当时,波音公司通过对许多重大故障与事故案例的研究,发现有许多故障与事故并不是由于元器件失效引起的,而是由于系统设计方案之中固有的状态引起的,而这些状态是设计者为了实现设计意图而无意带进设计方案中的。在这些状态下,系统存在着某些设计者未认识到的电回路,不同程度地传递着某种能量流、信息流或控制信号流。系统的有关部分一旦被这些潜流所激发,就会产生非预期的功能,或是抑制了预期的功能,引起系统故障,有时会造成严重事故,包括设备损坏和人员伤亡。例如,飞机在停机坪上误发具有严重危害性的核导弹;在座舱失火时不能迅速打开舱门逃逸,使宇航员遭到伤亡;火箭刚起飞又关机坐回发射台;测试中紧急断电却将发动机电爆管引爆;火箭发射中点火脱落插头提前脱落,使点火中断,发射失败等等。哪一起事故所造成的损失都是惊人的。不仅在经济上损失巨大,而且丧失了宝贵的时间,在政治上和军事上都造成巨大损失。研究证明,在复杂的气路、液路系统中也存在某些潜在路径(Sneak Path),同样具有严重的危害。潜在电路和潜在路径统称为潜在通路(Sneak Passage)。

① 收稿日期:1999-12-20
严殿启,男,研究员,主要研究方向为潜在分析技术应用

潜在分析技术是旨在预先发现潜在通路的一项工程技术，是一项具有特殊的社会经济效益的应用技术。

2 国外潜通路分析技术发展现状

美国阿波罗工程的决策者们认识到，要保证昂贵的设备及宇航员的安全，必须采取针对性措施，保证各个系统尤其是载人飞行器的各个系统具有足够高的安全性与可靠性。针对着潜在电路这种非失效相关的事故因素，于1967年投资于波音公司研究开发旨在预先发现潜在电路的潜在电路分析(Sneak Circuit Analysis，SCA)技术。经过8年的努力，取得很大的成功，建立了规范的潜在分析的理论与方法。并开发了计算机辅助工具。按这种理论和方法，首先是将一个复杂的无序的庞大系统图通过划分和简化转化为由节点和边(分支)组成的集。再通过具有遍历性的路径推导和追踪，生成体现系统连通性的网络树。进一步的研究还发现，这些网络树图形不外乎由5种基本拓扑图形组成。这就是直线型(I型)、电源拱型(Y型)、地拱型(倒Y型)、组合拱形(X型)和"H"型，如图1所示。

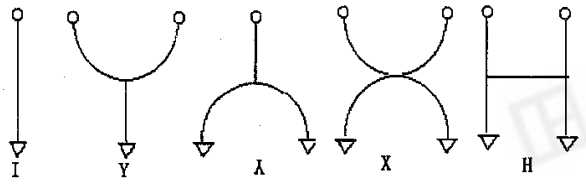

图1 5种基本拓扑图形

每种基本拓扑图形都有它特有的连通性行为，这些行为包含着某些设计期望行为和可能存在的非设计期望行为，也就是潜在通路。进行SCA分析时，就是要识别出系统各种运行状态下的相关网络树(多棵树称为网络森林)中所包含的拓扑图形，这样就较容易发现某些拓扑图形中的非期望行为。通过分析所有网络树中的所有的拓扑图形，潜通路也就暴露无遗了。

至1975年，波音公司完成了阿波罗的潜在分析任务，发现潜在电路208个，设计缺陷13个，设计图错误1 500个，提高了阿波罗的安全性与可靠性，在工程界产生了很大的反响，很快在各个重要领域得到应用。在完成阿波罗分析任务期间，还完成其他16项分析合同，包括军用系统6项，航天系统(含阿波罗)6项，工业/核装置系统5项。共发现潜在电路4 185个，设计缺陷740个，设计资料错误2 963个。

通过一段时间的实际分析，潜通路分析的内容得到了扩展。在非失效相关的故障因素中除了潜在通路外，还存在设计缺陷、设计资料(Data)错误两大类因素。这3类问题都属于非失效因素，统称为"潜在问题"。相应的分析技术也称为潜在分析(Sneak Analysis，SA)。当然，SCA技术仍然是SA的核心。

由于SA技术在预先发现潜在通路及潜在问题，从而有效地避免严酷度高、损失巨大的事故方面的特殊功效，1980年被作为军用系统设备可靠性和安全性保障措施之一，列入美军标准MIL-STD-785B中。也正是由于这种特殊而巨大的效益和高难度，SA技术一直被波音公司垄断保密，至今未曾公开有关的具体资料。

这种规范化分析的另一个特殊工具是被称之为线索表(Clue List)的经验知识库，它被用来作为分析时的提示。线索表是在调查收集大量的历史案例并加以深入的分析提炼而产生的经验性知识库。这种知识越全面、越丰富，对于分析的提示、引导作用就越全面、越准确，就越能彻底地发现所有潜在的问题。文献[1]透露，美国建起比较全面丰富的线索表用了15年时间，可见这项任务的艰巨。这个线索表是更为绝密的文献。由于上述情况，SCA技术一度被称为"黑色艺术"(Black Art)。

许多先进的国家对SA技术是十分重视的，已经普遍应用于复杂的电子电气系统、动力输送系统、软件、化工、港口指挥调度系统、核装置控制系统等关键系统的设计和可靠性分析中。随着应用的扩展，也出现了一些简化的SCA方法和应用系统。例如美国SoHaR公司的SCAT和欧洲宇航局的SNAP。

3 我国自行开发的通用潜在分析系统

3.1 工作原理

自1988年开始，一些研究所和高等院校都陆续

开展了研究工作。

经过几年的努力，自行开发的通用潜在分析系统(Conventional Sneak Analysis System，CSAS)已投入了重要工程应用。其主要组成和工作流程如图 2 所示。其中网络树生成、树图绘制都是由计算机辅助系统自动完成的。应用提示线索的分析是在树图界面上采用人机交互方式进行的。

连通性数据是合同委托方提供的被分析系统有关的反映系统连通性和运行状态的生产制造数据。

数据预处理是由人工进行的，按 CSAS 数据预处理规范提出网络树生成系统(Net Tree Generation System，NTGS)所需要的所有设置数据，同时提供树图生成系统(Tree Graph Generation System，TGGS)，以及在人机交互式分析中所必须的“功能森林表”。

NTGS 的数据录入用两种方式：对于用计算机辅助设计(CAD)提供的数据用网表转换工具箱(Net Table Transformation Tool Box，NTTTB)中与 CAD 相应的转换工具软件自动完成，而对于目前尚大量存在的手工设计数据用手工录入。

NTGS 主要功能是生成系统网络森林，并进而生成符合 TGGS 要求的网络树表和交叉参照表，并由网络树功能组织程序根据预处理提供的“功能执行分支表”生成功能森林表。

树图分析由 3 部分组成，如图 3 所示。

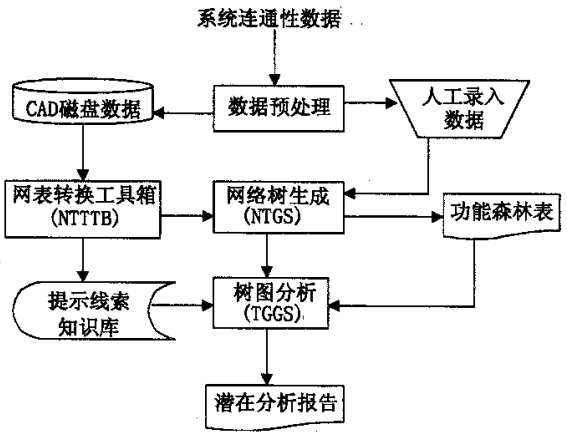

图 2　CSAS 主流程图

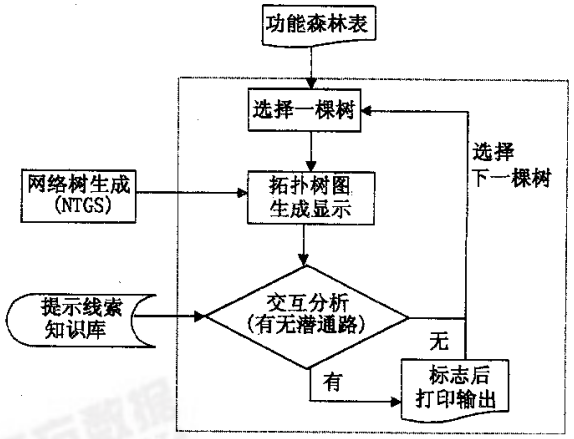

图 3　树图分析流程

提示线索知识库，它提供了分析树图的各种经验线索。

功能森林表，它提供各个功能的相关树(森林)表。

人机交互式分析过程，如虚线框出部分：选择某功能森林中的一棵树，用 TGGS 软件生成网络树图并显示在屏幕上，应用线索表中的有关线索，对于树中所包含的每个拓扑结构进行分析，若无潜在问题，则选择下一棵树重复上述分析过程，若有潜通路或设计错误、设计缺陷等，则在标志后打印输出，再选择一棵树进行同样的分析，直至分析完功能森林中的每一个功能的每一棵树。对于所有打印出的有潜通路(设计缺陷)标志的树图和其它界面上发现的设计缺陷、数据错误等潜在问题进行进一步校准确认并提出纠正措施建议后，编写成潜在分析报告，由任务委托方进行评审验收。

3.2　CSAS 提示线索表

3.2.1　线索表的组成和格式

CSAS 提示线索表由两类线索组成，即潜在通路线索和设计缺陷线索。采用如下格式：

S(D)Ci：第 i 条潜通路(或设计缺陷)线索的内容描述($i=1,2\cdots$)；

S(D)Ci.1：第 i 条潜通路(或设计缺陷)线索的

适用拓扑图形或电路元件；

S(D)Ci.2：第 i 条潜通路(或设计缺陷)线索相应的基本纠正措施；

S(D)Ci.3.n：第 i 条潜通路(或设计缺陷)线索的第 n 个案例($n=1,2\cdots$)。

3.2.2 线索表实例

SC1：信号线与其同一组的地线分别通过没有严格的时序控制的连接器时，在一定的时段里存在潜通路(潜在定时)。

SC1.1：I，Y，人，X，H。

SC1.2：使同一组信号线与地线通过同一个插头。

SC1.3.1：美国红宝石火箭在第 51 次发射时由于尾插头(TB)较脱落插头(TC)早断开 29 ms，使点火指示信号通过指示灯后又通过潜通路(紧急关机指示继电器线圈和抑制二极管、TC、关机线圈到地)，导致火箭刚起飞又被关机，掉回了发射台。拓扑网络树如图 4 所示。

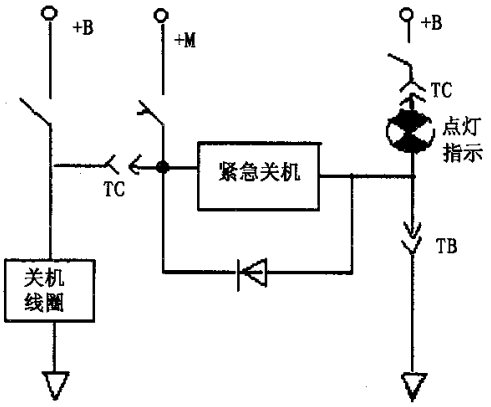

图 4 案例 SC1.3.1 拓扑网络树

DC1：并联分流电路，当各分支存在不等时动作时，可能导致各分支电路超载，从而降低可靠寿命。

DC1.1：继电器触点并联电路。

DC1.1：按单个支路承受总负载电流的标准选用每个支路的承载参数。

DC1.3.1：某控制设备中采用继电器并联电路控制直流电机的通断，如图 5 所示。在现场测试中发现直流电机断不了电，原因是 J1 触点烧结。烧结的原因是由于 J1、J2 的实际通断时间是不同的。对于电机这种感性负载来说，早接通的触点要承受全部启动电流。要求按 0.3 降额系数选用断路元件。电机额定电流为 6 A，J1、J2 触点额定电流为 12 A，而按降额 0.3 选择其单个支路承载参数，应为

$$6A \div 0.3 = 20\ A$$

也就是说应选用触点承载能力不小于 20 A 的继电器。

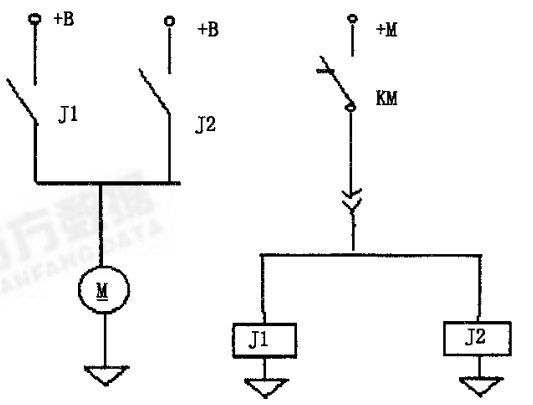

图 5 案例 DC1 拓扑网络森林

3.3 CSAS 的技术指标和应用效果

CSAS 目前可以完成分支总数为 100 000 个的系统 SA 任务。按平均每个元件 5 个分支计，折合 20 000 个元件，可以满足当前我国航天系统和其他关键系统的需要。

应用 CSAS 已经先后完成了 4 项任务，其规模和效果列于表 1。

在发现的潜通路问题中，有些危害度是相当高的，由于它们的被提前发现并采取了相应的措施，消除了这些潜在隐患，充分体现了 CSAS 的有效性和巨大社会经济效益。

表 1　CSAS 应用统计

任务代号	规模(元件数)	发现的各种潜在问题数			
		潜通路	设计缺陷	设计错误	设计资料错误
C	289	5	2	0	18
F	96	2	7	0	0
D	973	7	10	0	25
G	1 973	20	11	12	59
合计	3 331	34	30	12	102

3.4　CSAS 的发展方向

所说的发展方向并非指规范的 SA 或简化的 SA 问题，这个问题将随着计算机辅助水平的提高而消失。CSAS 的发展方向是如何减少人工劳动项目而最大限度地提高自动化、智能化水平的问题。根据应用体会，当务之急的问题是：

a）系统输入问题。这个问题需要与 CAD 技术的密切配合，在设计过程中建立公用数据库，与 CSAS 采用规范的协调一致的数据结构和相同的标识。这就如同邮电系统采用自动分拣技术必须要全体邮民在信封格式上采用统一的格式一样，解决由 CAD 数据自动转入 CSAS 的问题。最大限度地取代手工录入。

b）应用线索表知识自动完成分析的智能化算法和软件开发问题。

c）将潜在分析技术通过模拟仿真方法应用于非电气系统问题。

参　考　文　献

1　Buratti Davey L，Godoy Sylvia G. Sneak analysis application guidelines. Boeing Aerospace Company，1982-06.

2　Frank Ellis Y. Sneak circuit analysis automation. Bing Aerospace，Seattle.

3　严殿启. CSAS 的现在和将来.《航天控制》创刊 10 周年学术交流会文献，1998-06.