文章编号:1671-4598(2018)04-0011-04 DOI:10.16526/j.cnki.11—4762/tp.2018.04.004 中图分类号:TP391.41 文献标识码:A

电压频控中抗强干扰软件关联缺陷检测

刘 欣[1],张 楠[2],孙辰军[1]
(1.国网河北省电力公司,石家庄 050021;2.南京南瑞集团公司,南京 210000)

摘要:针对传统电压频控软件缺陷检测技术未考虑软件缺陷分类,存在检测精度低的问题,提出一种电压频控中抗强干扰软件关联缺陷检测技术;对软件关联缺陷检测原理进行分析,采用判别函数对待测软件样本进行识别,引入统计模式识别算法处理软件原始数据,依据关联缺陷概率分配,确定关联缺陷类别,计算缺陷特征值,利用贝叶斯分类器对关联缺陷进行划分,完成抗强干扰软件关联缺陷的分类,从而实现关联缺陷的高精度检测;实验结果表明,该检测技术对软件缺陷进行准确分类,在保证强抗干扰性的前提下,有效提高了检测精度。

关键词:电压频控;抗强干扰;软件缺陷;检测

Detection of Anti Strong Interference Software Associated Defects in Voltage frequency control

Liu Xin[1], Zhang Nan[2], Sun Chenjun[1]
(1. State grid hebei electirc power company, Shijiazhuang 050021, China;
2. Nari group corporation nanjing, Nanjing 210000, China)

Abstract: The traditional voltage and frequency control software defect detection technology does not consider the classification of software defects, and has the problem of low detection accuracy. The software defect correlation detection principle were analyzed using discriminant function test software to identify sample treatment, introduced statistical pattern recognition algorithm of original data processing software, based on defect correlation probability distribution, determine the associated defects of calculation of defect feature values to classify the defect correlation using Bayesian classifier, complete classification of anti interference software defect correlation in order to achieve high precision detection, defect correlation. The experimental results show that the detection technology can accurately classify the software defects and effectively improve the detection accuracy on the premise of ensuring strong anti-interference.

Keywords: voltage frequency control; anti strong interference; software defect; detection

0 引言

电压频率控制的实现常受线路阻抗的影响,难以达成有无功率的分配,且电压幅值与频率测量精度密切相关[1],因此设计大量电压频率控制软件对电压频率加以控制。随着电压频率控制软件大小呈指数增加,其关联缺陷问题逐渐引起人们的重视[2]。在软件开发中,对电压频控中抗强干扰软件的关联缺陷进行检测是一个不可忽略的环节,它关系到电压频控软件能否稳定运行[3]。当前的软件缺陷检测技术能够有效保障电压频控软件的强抗干扰性,但在检测过程中,因软件太大导致检测精度较低。因此,提出一种电压频控中抗强干扰软件关联缺陷检测技术,在保证强抗干扰性的同时,提高软件关联缺陷的监测精度。

1 软件关联缺陷检测原理

要研究一种电压频控中抗强干扰软件关联缺陷检测技术,需先对软件关联缺陷检测原理进行分析。给出电压频控中抗强干扰软件关联缺陷检测原理如图1所示。

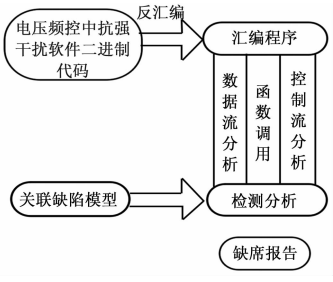


图1 软件关联缺陷检测原理图

将电压频控中抗强干扰软件的二进制代码输入关联缺陷检测,根据电压频控中抗强干扰软件的二进制代码汇编成对应的程序[4]。在该程序的基础上分析电压频控中抗强干扰软件的控制流、数据流和函数调用关系。得到分析结果进行电压频控中抗强干扰软件关联缺陷模型的构建,产生电压频控中抗强干扰软件的缺陷结果,并得到软件的缺陷报告。

经过以上分析,利用软件关联缺陷检测原理能够完成电压频控中抗强干扰软件关联缺陷检测技术的研究,使改进的检测技术具有一定的合理性和可行性。

2 关联缺陷的分类

依据软件关联缺陷检测原理,对电压频控中抗强干扰软件关联缺陷检测技术进行设计。充分分析致使传统检测技术检测

收稿日期:2018-01-16; **修回日期**:2018-02-08。
基金项目:国家电网公司总部科技项目(XX71—15—036)。
作者简介:刘 欣(1977-),男,河北石家庄人,硕士研究生,高级工程师,主要从事电力信息化、软件工程方向的研究。

精度低的原因，得出，传统检测技术未考虑关联缺陷的类别问题，使庞大的软件无法得到准确检测，因此，改进的电压频控中抗强干扰软件关联缺陷检测技术，首先针对软件的关联缺陷进行分类，以提高检测精度。具体过程描述如下：

统计模式识别算法是用来选择电压频控中抗强干扰软件的原始数据并进行软件原始数据处理的样本集，电压频控中抗强干扰软件关联缺陷检测技术采用判别函数对待测的软件样本进行识别，根据软件关联缺陷类型的不同进行识别分类。统计模式识别方法分为训练样本和识别两个阶段[5]，电压频控中抗强干扰软件关联缺陷检测技术的软件样本识别框图如图 2 所示。

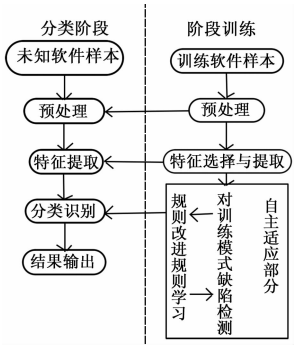


图 2 关联缺陷检测技术软件样本识别框图

电压频控中抗强干扰软件关联缺陷检测技术的训练软件样本阶段根据软件的关联缺陷特征完成关联缺陷的划分，使软件关联缺陷存在较好的区分线，并根据已知的关联缺陷类型制定判别规则，确保样本分析判别结果准确；分类阶段的主要目的是根据训练阶段的判别规则和缺陷特征进行比较，将软件关联缺陷归类模式，并进行关联缺陷的分类。

本文采用贝叶斯分类器对提取的软件关联缺陷进行分类[6]，贝叶斯分类器建立在三点假设之上。

1）已知软件关联缺陷概率的分配；

2）确定软件关联缺陷的类别；

3）得到的软件关联缺陷存在特征值和特征向量。

设 x 代表的是软件关联缺陷特征值，w 代表属于某缺陷的概率其中 $i=1,2,3$。L_{ij} 表示误差，代表属于 w_i 类的缺陷被分类器分类到 w_j。对关联缺陷特征值 x 进行判断时，贝叶斯分类器将 x 分类到三种关联缺陷中的一个，其出现误差的计算公式为：

$$r_j(x)=\sum_{i=1}^{3}L_{ij}w_i \tag{1}$$

$r_j(x)$ 被称为条件平均风险，为了确定关联缺陷特征值 x 的种类，需要对关联缺陷特征值 x 分到每种关联缺陷的条件平均风险进行计算，计算公式为：

$$r_i=\min\left|r_1(x),r_2(x),r_3(x)\right| \tag{2}$$

通过计算 r_i，确定软件关联缺陷的种类，提高电压频控中抗强干扰软件关联缺陷检测技术的检测精度。

根据以上步骤，能够实现电压频控中抗强干扰软件关联缺陷的准确分类，依据分类结果，将多种类别的关联缺陷分组进行检测，不仅加快了软件关联缺陷的检测速率，也是有效提高改进检测技术检测精度的关键所在。关联缺陷的分类过程为检测技术的实现奠定了良好的基础。

3 关联缺陷检测的实现

根据已经分类好的关联缺陷类型，采用反汇编的方式，对软件的数据流和各功能函数调用过程进行分析，改进软件的控制流，依据分析结果，并结合静态分析方法，建立关联缺陷检测模型，实现电压频控中抗强干扰软件关联缺陷的检测。具体实现过程描述如下：

1）反汇编：在电压频控中抗强干扰软件关联缺陷检测技术中反汇编的过程就是对汇编程序进行逆向汇编[5]。反汇编的主要功能是编辑在软件内执行的二进制代码的特征。为了标识和分解出软件数据代码和平台指令代码，需要对反汇编生成的二进制代码进行加工处理。最后将软件关联缺陷检测技术的指令代码反汇编成易于理解的文件。电压频控中抗强干扰软件关联缺陷检测技术的反汇编流程如图 3 所示。

图 3 关联缺陷检测技术反汇编流程图

2）数据流分析：电压频控中抗强干扰软件关联缺陷检测技术中二进制代码的数据流分析方法与软件的类型无关，分析电压频控中抗强干扰软件的数据流，可以减少软件关联缺陷分析的复杂度。对软件局部进行分析，得到的结果准确性较高，将数据流划分为若干个局部数据流，根据各组件分析得到的结果及软件输出和输入的数据，得到完整的软件数据流图。进行电压频控中抗强干扰软件关联缺陷检测时，使用数据流分析法需要软件执行流信息和数据流信息。数据流分析法的原理是跟踪软件序列、返回值和参数[7]，进行分析，判断软件是否存在关联缺陷。

3）函数调用：在对电压频控中抗强干扰软件关联缺陷进行检测的过程中，通过各功能函数完成检测技术的相关指令。各功能函数调用的具体过程为在关联缺陷检测过程中遇到需要跳转的地址，并进行保存。将关联缺陷检测过程的 PC 转入到对应的函数接口中，执行检测指令，最后跳转到保存之前的地址。在电压频控中抗强干扰软件关联缺陷检测过程中各功能函数的调用分为嵌套调用和一般调用，其中嵌套调用指的是一个功能函数中需要调用其他的功能函数。

本文采用反汇编技术进行各功能函数间调用，关联缺陷检测过程以反汇编为基础，而控制流中的跳转指令和分值指令秉持过程调用关系，从而保障电压频控软件的强抗干扰性能。

4）控制流改进：控制流改进是根据电压频控中抗强干扰软件关联缺陷检测程序的运行序列，在关联缺陷检测程序运行序列的基础上对软件的基本块进行划分，划分的内容根据过程间的控制流和过程内的控制流运行。过程间的控制流是对软件基本块之间的调用关系进行控制[8]，过程内控制流是对软件基本块内指令关系进行控制。控制流改进的具体过程是将软件关联缺陷检测程序中可执行的软件文件进行反汇编得到汇编程序，程序控制流通过对软件基本块的划分得到控制流图，通过分析调用得到检测过程的调用图如图 4 所示。

5）静态分析关联缺陷检测模型：采用静态分析工具对电压频控中抗强干扰软件进行缺陷检测，检测模型如下：

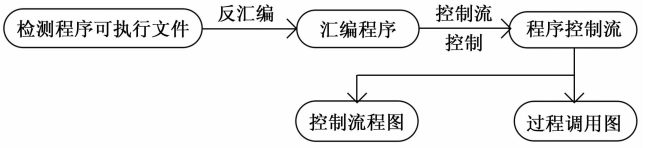


图 4　控制流控制过程调用图

（1）初始化及变量定义关联缺陷检测模型。检测电压频控中抗强干扰软件关联缺陷变量是否定义，判断该变量是否引用初始化或未定义的变量，检查是否存在未使用的赋值变量。建立软件相关变量的交叉引用实现。

（2）软件接口缺陷检测模型。检测平台程序在调用时实参和形参的数量和类别是否一致，平台输出和输入参数的定义是否匹配，软件的变量和外部变量是否相等。

（3）溢出缺陷检测模型。关联缺陷检测程序中的危险函数存在缺陷，对函数的边界进行检测。

（4）逻辑缺陷检测模型。进行关联缺陷检测程序的逻辑检查时，会出现不正确、不必要的结构代码。采用循环控制变量进行赋值，或存储软件其他模块的局部信息等。

在电压频控中抗强干扰软件关联缺陷检测技术中，静态缺陷检测可以准确地发现软件存在的关联缺陷，提高检测技术的检测精度。

综上所述，以软件关联缺陷检测原理为理论依据，采用贝叶斯分类器对软件中的关联缺陷进行分类，依据分类结果，充分分析软件的数据流及其函数调用过程，改进控制流，结合反汇编方式完善关联缺陷检测程序，从而实现电压频控中抗强干扰软件关联缺陷的检测。

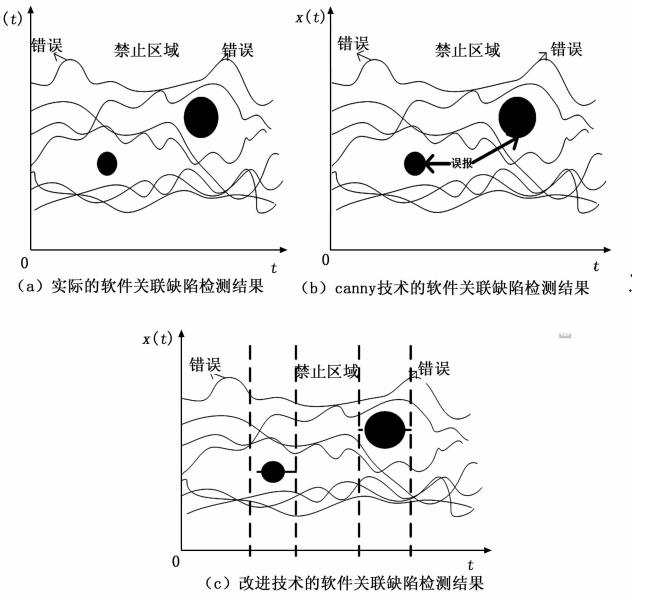
4　实验结果与分析

本次实验在 MATLAB 环境下完成，操作平台的系统为 32 位的 Windows7。为了验证电压频控中抗强干扰软件关联缺陷检测技术的有效性，对检测技术进行测试，图 5（a）为实际的软件关联缺陷检测结果，图 5（b）为基于 Canny 缺陷检测技术的软件关联缺陷检测结果，图 5（c）为改进技术的软件关联缺陷检测结果。

在图 5 中，曲线代表的是软件关联缺陷检测程序的运行踪迹，图中“禁止区域”表示的是缺陷模式所描述的安全属性，当一条检测程序的运动踪迹出现在“禁止区域”时，代表该软件存在一个关联缺陷，对比图 5（a）、图 5（b）与图 5（c），发现基于 Canny 技术的关联缺陷检测技术的检测结果与实际检测结果相比出现了两处误报；改进技术的软件关联缺陷检测结果与实际结果一致，验证了改进技术对电压频控中抗强干扰软件的关联缺陷进行检测时，检测结果较为精准。

通过参数 x 对电压频控中抗强干扰软件关联缺陷检测技术进行有效性测试，x 代表的是关联缺陷特征值，当关联缺陷特征值 x 越大时，关联缺陷越容易被检测出来，在相同的检测时间内，分别采用改进技术和基于层次模型的软件关联缺陷检测技术进行监测精度测试，测试结果如表 1 所示。

分析表 1 可知，改进技术的缺陷特征值 x 平均为 55，软件关联缺陷检测的平均监测精度为 92%，基于层次模型的软件关联缺陷检测技术中缺陷特征值 x 平均为 30，软件关联缺陷检测的平均监测精度为 72%。缺陷特征值 x 越大，缺陷越容易检测出来，检测精度越高，对比改进技术和基于层次模型的检测技术的实验结果可得，改进技术的软件关联缺陷检测精度更高，验证了改进技术的可行性。



（a）实际的软件关联缺陷检测结果　（b）canny技术的软件关联缺陷检测结果

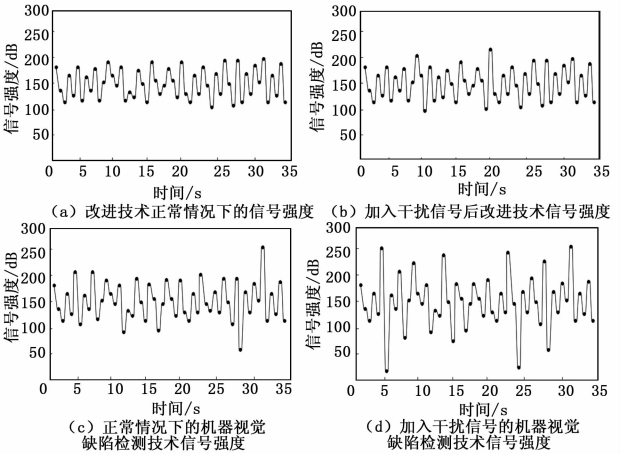
（c）改进技术的软件关联缺陷检测结果

图 5　两种不同技术的软件关联缺陷检测对比结果

表 1　两种不同技术相同检测时间内检测精度对比结果

实验序号	改进技术		层次模型的检测技术	
	x	检测精度/%	x	检测精度/%
1	50	90	30	72
2	45	88	20	68
3	60	92	40	70
4	65	95	30	75
平均	55	92	30	72

为了验证电压频控中抗强干扰软件关联缺陷检测技术在高精度检测的同时，能够保障其强抗干扰性，分别采用改进技术和基于机器视觉的关联缺陷检测技术进行抗干扰性能的测试，测试结果如图 6 所示。



（a）改进技术正常情况下的信号强度　（b）加入干扰信号后改进技术信号强度

（c）正常情况下的机器视觉缺陷检测技术信号强度　（d）加入干扰信号的机器视觉缺陷检测技术信号强度

图 6　两种不同技术的信号强度情况对比结果

图 6（a）为改进技术正常情况下的信号强度，图 6（b）

为加入干扰信号后改进技术的信号强度，对比图 6（a）和图 6（b）可知，改进技术的信号强度受到干扰信号的前后没有出现大规模的波动，信号强度保持平稳。图 6（c）为基于机器视觉的关联缺陷检测技术正常情况下的信号强度，图 6（d）为加入干扰信号后基于机器视觉的缺陷检测技术的信号强度，对比图 6（c）和图 6（d）可知，基于机器视觉的缺陷检测技术受到干扰信号前后的信号强度曲线出现了大规模的波动。对比两种技术的实验结果，可充分说明改进技术在检测过程中，依然保持其较强的抗干扰性能。

综合以上实验结果可得，改进的电压频控中抗强干扰软件关联缺陷检测技术，在保障其强抗干扰性能的前提下，具有较高的检测精度，验证了该技术的可行性和有效性。

5 结论

对电压频控中抗强干扰软件的关联缺陷进行检测，可以避免因软件关联缺陷造成的软件运行不稳定等潜在隐患，当前软件关联缺陷检测技术的检测结果存在检测精度低的问题，提出电压频控中抗强干扰软件关联缺陷检测技术。通过对关联缺陷进行准确分类，改进检测程序完成关联缺陷的精确检测。实验证明，该技术在保障强抗干扰性能的同时，具有较高的检测精度。未来将在检测速率方面进行深入研究，为软件缺陷检测领域的发展提供有效借鉴依据。

参考文献：

[1] 边伟成. 基于 AOP 的软件缺陷监测框架的设计与实现 [J]. 电子设计工程，2017（16）：27－31.

[2] 杨庆华，王 玲，荀 一，等. 基于机器视觉的袋泡茶包缺陷检测方法 [J]. 浙江工业大学学报，2015，43（2）：163－167.

[3] 郭 静，韩跃平，李会鸽. 产品表面缺陷检测的变步长采样机制研究 [J]. 科技通报，2017，33（2）：129－132.

[4] 刘学福，何小敏，许 亮，等. 基于显著性模型和区域生长法的药卷缺陷检测 [J]. 科学技术与工程，2015，15（4）：125－130.

[5] 钱 海，马小军，包仁标，等. 基于三维激光扫描和 BIM 的构件缺陷检测技术 [J]. 计算机测量与控制，2016，24（2）：14－17.

[6] 何博侠，张毅，童楷杰，等. 航天密封圈的曲面成像理论及其缺陷检测 [J]. 光学精密工程，2015，23（11）：3051－3060.

[7] 杨祖彬，代小红. 基于图像配准的食品包装印刷缺陷检测与实现 [J]. 计算机科学，2015，42（8）：319－322.

[8] 刘 亮，蒋 鑫，师普辛，等. 发电机出口电压互感器绝缘缺陷检测方法 [J]. 电网技术，2016，40（12）：3966－3972.

（上接第 11 页）

2）利用操纵杆操纵炮，加速减速，若随动半自动平稳，则随动半自动正常，检查方位受信仪是否夹紧，检查受信仪输出角度是否连续；

3）若随动半自动不平稳，检查功率放大板及相关电路。

在排故措施的指导下，快速定位故障单元为功率放大板，更换功率放大板后故障排除。

通过上述的分析及验证，采用这种 BIT 诊断为前导、故障案例推理为补充的结合方式能大大提高首次故障诊断率，降低无效排故时间，有效提高装备 BIT 和故障案例知识的利用效率。

装备 BIT 诊断、案例诊断以及两者融合诊断方法的优缺点分析如表 1 所示，通过比较可以看出 BIT 和案例融合的故障诊断方法综合了两种诊断方法的优点，有良好的推理能力和较高的故障诊断效率，能有效促进维修保障人员的现场诊断能力的提高。

表 1 故障诊断方法优缺点分析

诊断方法	优点	缺点
BIT 诊断	基于装备状态数据分析，诊断快速高效	虚警率较高，不具备推理和知识积累的能力，故障排除知识缺乏。
案例诊断	诊断过程直观，推理机制简单，故障排除方法明确	案例知识积累周期长，推理准确性依赖性强，但对新于故障案例有限的新型复杂装备，诊断能力不足。
BIT 与案例融合诊断	BIT 诊断与维修案例知识互为补充，推理效率高，容易得到正确的结论。	两种诊断方法融合的模式和机制有待完善。

4 结论

本文将基于 BIT 和案例融合的混合推理机制引入到装备故障诊断系统的设计中，以装备 BIT 诊断为前导，故障案例推理诊断后置补充的结合方式，构建了两者融合的推理模型，设计了基于 BIT 和案例融合的故障诊断系统。通过某新型火炮随动分系统的一诊断实例，比较分析了本文诊断方法与单独的 BIT 诊断和故障案例方法的优缺点。研究表明，基于 BIT 和案例融合的故障诊断方法，能够综合了两种诊断方法的优点，具有良好的推理能力和较高的故障诊断效率，能够有效提高维修保障人员对复杂装备的故障诊断能力。

参考文献：

[1] 谢永成，董今朝，李光升，等. 机内测试技术综述 [J]. 计算机测量与控制，2013，21（3）：550－553.

[2] 吕 隽，刘维罡. 导弹武器测试性设计与 BIT 技术 [J]. 战术导弹技术，2015（3）：46－50.

[3] 胡良明，徐 诚，李万平. 基于案例推理的自行火炮故障诊断专家系统 [J]. 火炮发射与控制学报，2006（2）：53－57.

[4] 张耀辉，李 浩，李林宏，等. 基于案例推理的装甲装备故障诊断方法 [J]. 兵工自动化，2014（9）：21－22.

[5] 柳 玉，贲可荣. 案例推理的故障诊断技术研究综述 [J]. 计算机科学与探索，2011，5（10）：865－879.

[6] 温熙森，徐永成，易晓山，等. 智能机内测试理论与应用 [M]. 北京：国防工业出版社，2002.

[7] 张 超，马存宝，宋 东，等. 智能机内测试研究综述 [J]. 计算机测量与控制，2007，15（2）：141－144.

[8] Lawanna A. An effective model for case－based maintenance in cased－based reasoning systems [A]. International Conference on Intelligent Informatics and Biomedical Sciences [C]. IEEE，2016：129－134.

[9] 李小青. 基于案例推理的故障诊断方法 [J]. 计算机测量与控制，2007，15（9）：1130－1131.