文章编号:1671-4598(2019)04-0097-05 DOI:10.16526/j.cnki.11—4762/tp.2019.04.023 中图分类号:TP806+.1 文献标识码:A

测试性验证试验的故障注入方法优化研究

颜世刚[1]，齐亚峰[2]
(1. 中国人民解放军 92941 部队 41 分队，辽宁 葫芦岛 125001；
2. 中国人民解放军 92941 部队 43 分队，辽宁 葫芦岛 125001)

摘要：测试性验证试验是舰炮制导弹药测试性水平的主要验证手段，故障注入是验证测试性水平的一种有效方法；舰炮制导弹药封装严密，故障注入难度大，导致部分故障模式无法实现和故障覆盖率较低，如何进行故障注入方法的优化和减少故障注入的成本成为亟待解决的问题；从某型舰炮制导弹药的故障模式分析出发，研究了其故障传递特性，利用故障传递特性建立故障与状态、故障与故障之间的关系，并运用贝叶斯网络多树传播算法得到了测试性等效故障相关矩阵，使用等效故障代替无法注入的故障，有效提高了故障的覆盖率，优化了测试性故障注入方法，完善了测试性验证试验；最终使测试性验证试验更加完备，测试性水平的验证结果可信度更高，实现了某型舰炮制导弹药主要故障模式的全部覆盖。

关键词：舰炮制导弹药；测试性验证试验；故障注入；故障传递；方法优化

Research on Optimization of Fault Injection Method for Testability Verification Test

Yan Shigang[1], Qi Yafeng[2]
(1. Unit 41 of 92941 Troops, PLA, Huludao 125001, China;
2. Unit 43 of 92941 Troops, PLA, Huludao 125001, China)

Abstract: The testability verification test is a main verification means to verify testing level of the guided projectile for naval guns, fault injection is a effective method to verify testing level, the guided projectile for naval guns is tightly packaged, fault injection is difficult, some fault modes can not be realized and fault coverage is low, how to optimize the fault injection method and reduce the cost of fault injection has become an urgent problem to be solved. The fault transfer characteristic is studied from the fault mode of a certain guided projectile for naval guns, the relation is established between fault and state, fault and fault by using fault transfer characteristics, the test equivalent fault correlation matrix is obtained by using Bayesian network multi-tree propagation algorithm, it can effectively improve the coverage of faults, and optimize the injection method of testability fault, and perfect the testability verification test by using equivalent fault instead of injectable fault. Finally, it makes the testability verification test more complete and the testability level verification results more reliable, the main fault modes of a guided projectile for naval guns are covered completely.

Keywords: guided projectile for naval guns; testability verification test; fault injection; fault propagation; method optimiization

0 引言

随着舰炮制导弹药的发展，其测试性作为质量监测的重要特性，以及维修保障性能的主要设计特性之一，越来越引起使用方和承制方的重视。测试性验证试验是舰炮制导弹药测试性水平的主要验证手段，故障注入作为验证测试性水平的一种有效方法，受到国内外研究人员的高度重视，如何进行故障注入方法的优化和减少故障注入的成本成为亟待解决的问题。故障注入是指人为地产生故障，以加速系统出现错误或失效，其方法一般分为基于硬件的故障注入、基于软件的故障注入和基于仿真的故障注入。以上三种方法各有优劣，直接对硬件进行故障注入虽然获得结果相对真实，但会对装备造成损伤；软件故障注入成本较低，而且不会对装备造成损伤，但是可实现的故障有限；基于仿真的故障注入虽然可以解决故障注入量的问题，但准确性不高、可信度差。

工程研究人员开发了大量的故障注入系统，用于验证装备或系统的可靠性和容错性。韩国航空大学提出了基于 System C 运行高效的混合故障注入环境 SyFI[1]。Jin-fu Chen[2]等提出了一种基于故障注入模型的测试策略，可有效检测组件漏洞，且故障检测率大于 90%。Shao C[3]等提出了一种针对故障注入的加密电路安全测试方法，实验结果证明了该方法的有效性。Wang G H[4]等建立了一种基于故障注入的可测试演示平台，能提高测试性验证试验的效率。Arasteh B[5]等提出了一种基于使用遗传算法的软件故障注入方法，比随机注入的结果更稳定、更准确。Yang C[6]等提出了一种引传动控制系统安全检测与故障诊断的故障注入策略。Wu J[7]等提出了一种混合故障注入模型，评估了故障预测模型。Li H[8]等提出了一种等效故障选择方法，解决了测试性试验中部分故障模式不能注入的问题，

收稿日期:2019-01-21； **修回日期**:2019-02-15。

作者简介:颜世刚(1972-),男,山东泰安人,硕士,高级工程师,主要从事舰载防空导弹系统、舰炮武器系统试验及仿真方向的研究。

对比等效故障和原故障发现此等效故障选择方法是可行的。Cui X[9]等运用 ATPG 方法得到了寻找最优等效故障模式的方法。陈然[10]等提出基于层次模型的可更换模块故障注入方法，有效解决了测试性验证试验中故障不可充分注入的问题。江建慧[11]分析了故障传递特性，并深入研究了故障传播机理。针对关联复杂系统的故障诊断问题，宋志平[12]等提出了用状态关联矩阵建立状态树，对故障传递特性进行补充。陈杰[13]等提出了一种基于故障传递矩阵的故障隔离方法，有效解决了复杂系统故障诊断的问题。李天梅[14]等分析了故障之间的传递特性，运用贝叶斯信度传播算法理论，提出了位置不可访问的故障注入方法，提高了故障覆盖率。

由于某些条件的约束和资源的局限，某型舰炮制导弹药仍然存在部分故障无法注入的情况，无法满足故障覆盖率要求，使测试性验证和评估结果的可信度受到质疑，严重影响使用方对装备测试性水平的掌握。鉴于此，本文分析了故障的传递特性，建立了故障与状态、故障与故障之间的关联关系，运用 Bayes 多树信度传播算法得到了测试性等效故障相关矩阵，使用等效故障代替无法注入的故障，提高了故障覆盖率，完善了测试性验证试验。

1 故障注入方法优化分析

由于某型舰炮制导弹药存在部分故障无法注入的问题，因此可通过研究故障传递特性，得到测试性等效故障，然后用等效故障代替无法注入的故障，提高故障覆盖率。

1.1 故障与状态间的关系

根据被试装备研制总要求规定的测试性指标，按照 GJB2072－94[15]等相关标准规定的试验方法进行测试性考核，当自然故障样本量不足时，须采用模拟故障的方式，以满足样本量需要。假设从某型舰炮制导弹药的故障样本中抽取 n 个故障模式进行故障注入，组成故障集 F。

$$F=\{f_1,f_2,\ldots,f_i,\ldots,f_n\} \tag{1}$$

UUT 的状态由 m 个信号参数组成，用向量 V 表示：

$$\boldsymbol{V}=\{v_1,v_2,\ldots,v_i,\ldots,v_m\} \tag{2}$$

得到故障与状态的相关矩阵 $\boldsymbol{R}_{FV}$ 如下：

$$\boldsymbol{R}_{FV}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1j} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2j} & \cdots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{i1} & r_{i2} & \cdots & r_{ij} & \cdots & r_{im} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nj} & \cdots & r_{nm} \end{bmatrix}_{n\times m} \tag{3}$$

式（3）中，r_{ij} 表示故障与状态参数之间的相关性，取值为 1 或 0。当 $r_{ij}=1$ 时，该故障的发生会引起状态参数突变；当 $r_{ij}=0$ 时，则相反。

1.2 故障间的相关性分析

由于系统各部件之间联系紧密，一个部件的故障必然会引起其状态信号异常，可能导致下一个或几个相邻部件同时发生故障，因此，故障是具有传播特性的。通过故障所对应的故障状态信号分析，可以得到基于测试性的等效故障矩阵 $\boldsymbol{E}_{FF}$：

$$\boldsymbol{E}_{FF}=\begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1j} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2j} & \cdots & e_{2k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{i1} & e_{i2} & \cdots & e_{ij} & \cdots & e_{ik} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{n1} & e_{n2} & \cdots & e_{nj} & \cdots & e_{nk} \end{bmatrix}_{n\times k} \tag{4}$$

式（4）中，e_{ij} 代表故障 f_i 与故障 f_j 之间的等效关系，取值为 1 或 0。当 $e_{ij}=1$ 时，表示两个故障引起的状态变化相同，那么故障 f_i 是故障 f_j 的一个等效故障；当 $e_{ij}=0$ 时，则两个故障不是等效故障。

为了进一步描述故障与状态、故障与故障之间的准确关系，需要确定矩阵 $\boldsymbol{R}_{FV}$ 和 $\boldsymbol{E}_{FF}$ 中元素的值。$\boldsymbol{R}_{FV}$ 可通过模糊概率 Petri 网[16]以及相关算法得到。由于某型舰炮制导弹药结构复杂，故障之间的关系相对复杂，存在很多不确定因素，需要借助贝叶斯网络多树传播算法确定 $\boldsymbol{E}_{FF}$。

2 贝叶斯网络多树传播算法

多树传播算法是指在贝叶斯网络中每处节点分配一个处理器[17]，综合相邻节点传递的故障信息以及处理器内部的条件概率信息进行计算，求出各节点的后验概率值，然后按照此规律继续传播。

假设在贝叶斯网络中，各变量取值为 1 或 0，其中“1”表示发生故障或处于故障状态，“0”表示未发生故障或处于正常状态。节点 B 可表示为有限集 $B=(B_1,B_2)$，且 B_1 与 B_2 互斥，其中 $B_1=1,B_2=0$。$B_i(i=1,2)$ 的信度计算公式如下：

$$BEL(B_i)=\tau\varphi(B_i)\theta(B_i) \tag{5}$$

式（5）中，τ 为满足 $\sum_{i=1}^{2}BEL(B_i)=1$ 的归一化因子。$\varphi(B_i)=P(C_B^-\mid B_i)$，$C_B^-$ 表示节点 B 的子节点对 B_i 的支持；$\theta(B_i)=P(B_i\mid C_B^+)$，其中 C_B^+ 表示节点 B 的父节点对 B_i 的支持。

定义 1：故障行为状态向量（$\boldsymbol{BC}$）

在 1.1 节中的矩阵 $\boldsymbol{R}_{FV}$ 中的第 i 行中所有取值为 1 的元素组成的向量组成故障 f_i 对应的行为状态向量 $\boldsymbol{BC}_i$。

在网络推理中，修改节点 B 的信度大小时需要考虑其父节点 A 的传递信息 $\theta_B(A)$ 以及各子节点的传递信息 $\varphi_1(B),\varphi_2(B),\cdots$

$$\begin{cases}\varphi_B(A)=\prod\limits_s\varphi_s(B_i)\\ \theta(B_i)=\mu\sum\limits_j P(B_i\mid A_j)\theta(A_j)\end{cases} \tag{6}$$

式（6）中，μ 为归一化因子。在贝叶斯网络传递中，信度可传递给子节点和父节点，从子节点 B 自下而上传递给其父节点 A 的信息如式（7）：

$$\varphi_B(A_j) = \prod_s \varphi_s(B_i) \sum_i P(B_i \mid A_j)\varphi(B_i) \tag{7}$$

从父节点 A 自上而下传递给子节点 B 的信息如式（8）：

$$\theta_E(B_i) = \pi\theta(B_i) \prod_k \varphi_k(B_i) \tag{8}$$

先按照式（7）计算自下而上向父节点传递的信息为 φ，然后根据式（8）计算自上而下向子节点传递的信息 θ，按照此方法计算全部节点的信息，根据式（5）可计算得到各故障节点的信度值。如果计算得到的信度值高于其先验值，则求解此故障对应的行为状态向量 $\boldsymbol{BC}_i'$，并与已经得出的行为状态向量 $\boldsymbol{BC}_i$ 对比，如果满足 $\boldsymbol{BC}_i = \boldsymbol{BC}_i'$，则两个故障互为等效故障，且在等效矩阵 $\boldsymbol{E}_{FF}$ 中的对应元素为 1；相反，则对应元素为 0。根据以上的方法进行多次计算，可得到故障等效矩阵 $\boldsymbol{E}_{FF}$。那么，等效故障也能清晰地在矩阵 $\boldsymbol{E}_{FF}$ 上反映出来。

3　案例分析

3.1　某型舰炮制导弹药主要故障模式分析

根据大量试验数据显示，发现射击试验的主要故障是近弹（未达到目标所在位置提前掉地），成为试验失败的主要原因[18]。制导弹药首次投入战争是在 1991 年的海湾战争，由于探测器件、惯性器件、电子器件、控制器件及动力装置等部分结构复杂，在快速发展和受到广泛关注的同时也暴露出一些问题。

故障树分析（fault tree analysis，FTA）是系统可靠性分析和故障诊断的一种有效方法。将某型舰炮制导弹药的故障现象进行故障树分析，得到导致这一现象的具体故障模式，作为改进弹药性能的重要参考，进一步提升其可靠性与作战效能。具体如图 1 所示。

3.2　电动舵机系统 FMECA 分析

故障模式、影响和危害性分析（failure mode，effects and criticality analysis，FMECA）一般根据工程实践与总结得到。分析各子系统或子单元的故障模式对装备或系统的影响，得到装备系统性的故障列表，发现设计中的重要单元和薄弱环节，用于改进装备的设计。

电动舵机系统作为某型舰炮制导弹药的主要功能部件，在控制炮弹飞行弹道和增加射程方面具有举足轻重的作用。经过理论分析和调研实践，得到其 FMECA 分析如表 1 所示。

3.3　基于硬件和软件的混合故障注入

根据 3.1 节中某型舰炮制导弹药的故障模式分析，从故障样本中抽取了主要的故障模式进行注入，具体情况如表 2 所示：

表 2 中“成功隔离次数”指故障被准确隔离到 LRU 的次数，根据表中数据显示，基于硬件和软件实现的故障注入总次数为 154 次，被成功检测且隔离的次数为 119 次。此外，存在 3 个故障模式无法注入，测试的覆盖率为 77.3%，故障注入率为 85.7%，难以满足测试性验证的要求。

3.4　运用贝叶斯网络多树传播算法求解等效故障

前面介绍了贝叶斯网络多树信度传播算法，这一节以某型舰炮制导弹药各子系统的故障模式为例进行分析和计算。

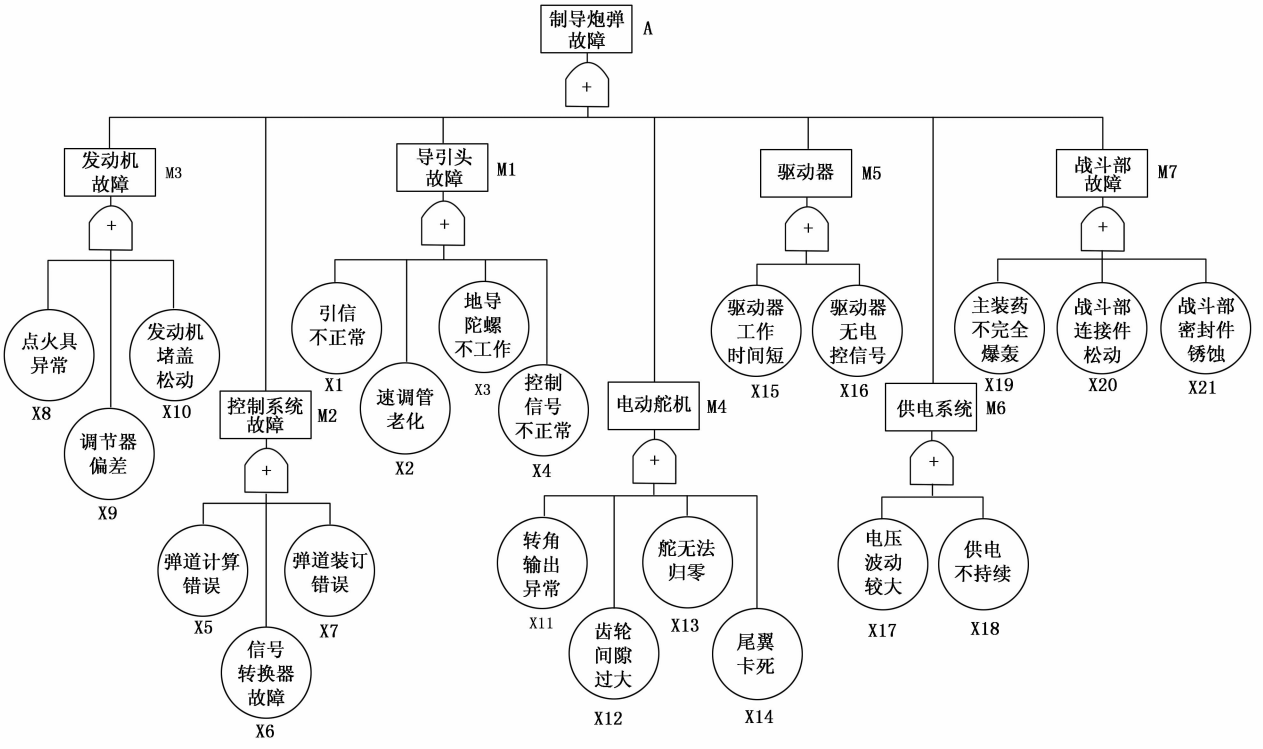

图 1　某型舰炮制导弹药故障树分析

表 1 某型舰炮制导弹药电动舵机 FMECA 分析

功能模块	功能	故障模式	故障原因	影响	检测方法
24V 直流电源	提供 24V 电压	无电压输出或电压过高或过低	线路或接地端电阻损坏	舵机系统无法正常工作	电压值测量
控制驱动器	接收弹载计算机的控制信号,驱动电动机转动	电机不按照指令转动	控制电缆断路或控制模式出错(选择位置控制模式)	无法按照控制指令驱动电机	检查电缆和控制模式设置
直流无刷电机	为舵机系统提供扭矩	扭矩或转速异常	控制参数选用不当或绕组损坏	舵效降低,系统滞后	控制参数调整或电流和电阻值测量
舵片张开锁定机构	打开和固定舵片	舵片抖动或卡死	装配异常或结构尺寸超差	舵片无法张开或转动	观察装配间隙
减速器	扭矩传递	减速器打滑或转动不均匀	安装配合不精密	扭矩输出不正常	观察和尺寸检测
反馈电位器	反馈舵片偏转角度	电位器反馈信息不稳定	电位器磨损、接触不良或短接	反馈异常,影响准确判断	电阻值测量和线性度测量

以表 2 中电动舵机的“齿轮间隙过大 f_1”、“轮齿断裂 f_2”和“轴承失效 f_3”三个的常见故障模式进行分析,这三个故障对应的主要状态信号为“转速信号 g_1”、“噪声信号 g_2”、“振动信号 g_3”和“温度信号 g_4”。根据试验数据和专家经验得出故障与信号的关系如图 2 所示。

表 2 某型舰炮制导弹药故障模式混合注入

子系统	故障模式	故障注入次数	成功检测次数	成功隔离次数	故障注入方式
电动舵机	齿轮间隙过大 f_1	*	*	*	无法注入
	轮齿断裂 f_2	9	8	7	硬件注入
	无法归零 f_3	9	8	7	硬件注入
	轴承失效 f_4	10	9	8	软件注入
导引头	引信不正常 f_5	7	6	6	硬件注入
	位姿漂移 f_6	*	*	*	无法注入
	惯导陀螺异常 f_7	9	8	7	硬件注入
	控制信号异常 f_8	9	8	7	软件注入
制导系统	弹道计算错误 f_9	8	8	6	软件注入
	信号转换器故障 f_{10}	8	7	6	软件注入
	弹道装定错误 f_{11}	10	9	8	软件注入
发动机	点火具异常 f_{12}	7	6	5	硬件注入
	调节器偏差 f_{13}	7	7	5	硬件注入
	发动机堵盖松动 f_{14}	8	6	6	硬件注入
驱动器	工作时间短 f_{15}	10	9	8	硬件注入
	无电控信号 f_{16}	9	9	7	软件注入
供电系统	电压波动较大 f_{17}	10	9	8	软件注入
	供电不持续 f_{18}	10	9	8	硬件注入
战斗部	装药密度不均匀 f_{19}	7	6	5	硬件注入
	连接件松动 f_{20}	7	7	5	硬件注入
	不能完全爆轰蚀 f_{21}	*	*	*	无法注入

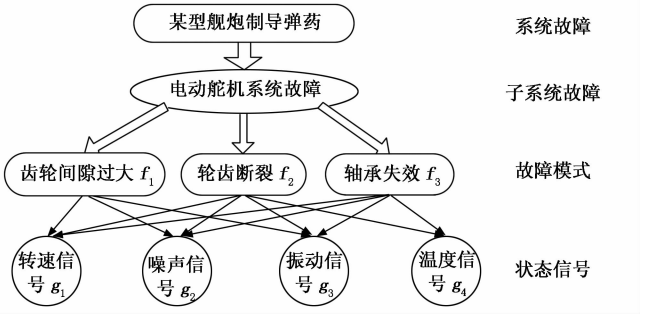

图 2 故障模式与状态信号的关系

在试验信息的基础上得到贝叶斯推理的故障概率信息如下:

$$P(g_1 \mid f_1) = \begin{bmatrix} 0.80 & 0.20 \\ 0.20 & 0.80 \end{bmatrix} \tag{9}$$

$$P(g_2 \mid f_1) = \begin{bmatrix} 0.40 & 0.60 \\ 0.60 & 0.40 \end{bmatrix} \tag{10}$$

$$P(g_3 \mid f_1) = \begin{bmatrix} 0.70 & 0.30 \\ 0.30 & 0.70 \end{bmatrix} \tag{11}$$

$$P(g_4 \mid f_1) = \begin{bmatrix} 0.60 & 0.40 \\ 0.40 & 0.60 \end{bmatrix} \tag{12}$$

假设故障 f_1 为已知的故障节点,且故障率为 0.70,根据信度传递中贝叶斯条件概率计算得到各状态节点的信度大小如表 3 所示。

从表 3 中可以看出,在故障 f_1 发生时,转速信号 g_1 和噪声信号 g_2 的故障信度超过了阈值。根据专家经验得到的贝叶斯反向推理网络的条件概率如下:

表 3　各状态节点信度大小和信度阈值

状态节点	g_1	g_2	g_3	g_4
正常信度	0.28	0.21	0.35	0.60
故障信度	0.72	0.79	0.65	0.40
信度阈值	0.70	0.70	0.70	0.70

$$P(g_1 \mid f_2)=\begin{bmatrix}0.2 & 0.8\\ 0.8 & 0.2\end{bmatrix} \tag{13}$$

$$P(g_1 \mid f_3)=\begin{bmatrix}0.4 & 0.6\\ 0.6 & 0.4\end{bmatrix} \tag{14}$$

$$P(g_2 \mid f_2)=\begin{bmatrix}0.9 & 0.1\\ 0.1 & 0.9\end{bmatrix} \tag{15}$$

$$P(g_2 \mid f_3)=\begin{bmatrix}0.6 & 0.4\\ 0.4 & 0.6\end{bmatrix} \tag{16}$$

假设在转速信号 g_1 和噪声信号 g_2 的出现异常的概率均为 0.70，经过信度传递算法计算得到各故障节点的信度大小如表 4 所示。

表 4　各故障节点信度大小和阈值

故障节点	f_2	f_3
正常信度	0.21	0.40
故障信度	0.79	0.60
信度阈值	0.70	0.70

在转速信号 g_1 和噪声信号 g_2 的出现异常的情况下，f_2 故障信度大于阈值，而且在故障 f_2 发生时，信号 g_1 与 g_2 也处于非正常状态。从而可以判断 f_2 是 f_1 的一个等效故障，从而可用故障 f_2 代替故障 f_1，解决故障 f_1 无法注入的问题。

同理，根据贝叶斯网络多树传播算法可得到故障模式 f_7 和 f_{19} 分别是故障模式 f_6 和 f_{21} 的等效故障，通过等效故障代替无法注入的故障模式，可将故障覆盖率从 85.7% 提高至 100%，从而优化了故障注入方法。

4　结论

本文针对某型舰炮制导弹药封装严密，故障注入难度大，导致部分故障模式无法实现和故障覆盖率较低的问题，利用故障传递特性得到故障与状态、故障与故障之间的关系，并运用贝叶斯网络多树传播算法求解等效故障，最终实现了某型舰炮制导弹药主要故障模式的全部覆盖，使测试性验证试验更加完备，测试性水平的验证结果可信度更高。

参考文献：

[1] Lee D W, Na J W. A Novel Simulation fault injection using electronic systems level simulation models [J]. IEEE Design&Test of Computers, 2009 (99): 1-1.

[2] Chen J F, Lu Y S, Zhang W, et al. A fault injection model—oriented testing strategy for component security [J]. Journal of Central South University, 2009, 16 (2): 258-264.

[3] Shao C, Li H, Zhou J. Fast and automatic security test on cryptographic ICs against fault injection attacks based on design for security test [J]. Iet Information Security, 2017, 11 (6): 312-318.

[4] Wang G H, Qin W J, Zhang W S. A testability—demonstration software platform based on fault injection [A]. International Conference on Electronics, Electrical Engineering and Information Science [C]. 2016: 669-681.

[5] Arasteh B. A program—aware fault—Injection method for dependability evaluation against soft—error using genetic algorithm [J]. Journal of Circuits Systems & Computers, 2018: 1850144.

[6] Yang C, Yang C, Peng T, et al. A fault—injection strategy for traction drive control systems [J]. IEEE Transactions on Industrial Electronics, 2017, PP (99): 1-1.

[7] Wu J, Jia X X, Liu C, et al. Finds in Testing Experiments for Model Evaluation [J]. Tsinghua Science & Technology, 2005, 10 (3): 298-303.

[8] Li H, Liu G, Yong Z. A method of equivalent fault selection based on extended dependency model [A]. Prognostics and System Health Management Conference [C]. IEEE, 2016: 1-5.

[9] Cui X, Qian Z, Shi X, et al. Test pattern generation for static burn—in based on equivalent fault model [A]. Electron Devices and Solid—State Circuits [C]. IEEE, 2013: 1-2.

[10] 陈　然，连光耀，秦子龙，等. 基于层次模型的外场可更换模块故障注入方法 [J]. 浙江大学学报（工学版），2017，51 (7)：1390-1396.

[11] 江建慧，吴捷程，孙　亚. 一种基于异常控制流的错误程序行为分析方法 [J]. 同济大学学报（自然科学版），2018，46 (7)：972-981.

[12] 宋志平，李应红. 状态关联及其在故障树自动建造中的应用 [J]. 航空发动机，2004，30 (3)：49-51.

[13] 陈　杰，戴文战. 基于故障传递概率的故障源位置诊断方法 [J]. 厦门大学学报（自然版），2001，40 (z1)：58-62.

[14] 李天梅，胡昌华，周　鑫. 基于故障传递特性的位置不可访问故障注入方法 [J]. 航空学报，2011，32 (12)：2277-2286.

[15] GJB2072—94，维修性试验与评定 [Z]. 国防科学技术工业委员会，1994.

[16] 李天梅，邱　静，刘冠军，等. 基于故障扩散强度的故障样本选取方法 [J]. 兵工学报，2008，29 (7)：829-833.

[17] 陆宁云，何克磊，姜　斌，等. 一种基于贝叶斯网络的故障预测方法 [J]. 东南大学学报（自然科学版），2012，42 (s1)：87-91.

[18] 刘建平. 激光末制导弹药故障分析 [J]. 弹箭与制导学报，2007，27 (5)：125-127.