《装备测试性工程系列丛书》序

现代装备功能与性能越来越先进，技术与结构越来越复杂，对装备测试、诊断与维修保障的挑战越来越严峻。传统的以外部测试为主的测试模式已无法从根本上解决复杂装备的测试问题。要实现准确、快速、全面的测试，就必须按照并行工程与集成科学的思想，在装备论证、设计与研制开始时就综合考虑测试与诊断问题。测试性工程作为装备“五性”工程的主要内容之一，正是应对这种变革与思想，旨在实现装备测试与诊断能力的“优生”和“优育”的总体优化，是从根本上提高装备测试与诊断水平的技术途径，也是当前国内外装备保障领域研究与应用的热点之一。

测试性概念和技术自 20 世纪末进入我国，在我国装备管理、研制部门和科研工作者的高度重视与共同努力下，取得了长足发展。部分新型装备明确提出了测试性要求，开展了测试性工程实践，积累了一定的测试性工程经验。

从总体上来看，我国装备测试性工程还处于以经验、规则为主导的阶段，严格按照有关国军标规范、系统科学地开展测试性论证、设计、分析与验证的案例还较少。从技术发展看，装备测试性工程已经从经验设计阶段发展到基于模型的科学设计阶段。相关部门也正组织编撰新标准，替代现行的 GJB 2547—95《装备测试性大纲》，旨在以基于模型的测试性分析与设计理论为指导，系统科学地开展装备测试性工程。

国防科学技术大学装备综合保障技术重点实验室在学科学术带头人温熙森教授、邱静教授的带领下，自“九五”以来一直致力于测试性领域的学术研究与工程应用，在智能机内测试、机内测试降虚警、测试性建模与分析、测试性设计、测试性验证与评估等方面取得了丰硕的研究与应用成果。《装备测试性工程系列丛书》正是对其最新研究成果的全面总结和体现。该丛书以测试性新标准为指导，结合典型案例，系统而全面地阐述了测试性工程的技术流程、测试性建模分析理论、测试性设计方法、测试性验证与评估技术等，并重点针对该领域存在的国际性难题——机内测试虚警问题，阐述了机电系统机内测试降虚警技术。

该丛书体系完整、结构清晰、理论深入、技术全面、方法规范、案例翔实，融系统

性、理论性、创新性和指导性于一体。我相信该丛书必将为测试性领域的管理与技术工作者提供非常好的参考和指导，对推动我国装备测试性工程发展也将起到积极的促进作用。

中国工程院院士

2011 年 12 月于北京

前　言

测试是装备使用和保障的信息源。装备的快速发展、实战化的使用要求和保障模式的变革，对装备测试诊断提出了更高的要求和更大的挑战。在研究和工程实践中发现：高新技术装备结构密集性和技术复杂性相对于现役装备显著增加，故障机理和表现更为复杂，状态信息的获取途径严重受限，传统的在使用后附加外部测试系统的模式无法从根本上解决这些复杂装备所面临的测试问题，测试模式的变革势在必行。

测试性，又称可测性，是指装备能及时准确地确定其状态（可工作、不可工作或性能降低），并隔离其内部故障的一种设计特性。装备测试性工程正是一种测试模式的变革。它按照并行工程的思想，在装备论证阶段就统筹考虑其测试诊断问题，通过与装备性能并行设计，使之具有良好的自测试和整体综合测试能力，实现装备测试能力的“优生”和测试的总体优化，从而快速、全面和准确地感知装备技术状态，实现装备快速智能检测、诊断与维修保障。良好的测试性设计对于提高装备的维修保障水平和战备完好性、降低全寿命周期费用等具有重要意义。

近年来，测试性作为装备的一个重要特性越来越受到重视，订购方对飞机、导弹、雷达等新型装备提出了明确的测试性指标要求。随着装备测试性工程的推进，如何发现测试性设计不足、指导测试性改进，如何判断装备的测试性指标是否达到合同规定的要求，如何给出订购方和承制方都认可的合理评价，成为装备面临的现实问题，也正是开展测试性试验与评价工作的意义所在。

20 世纪 80 年代以来，测试性试验与评价技术在国内外取得了一些成果和应用，也发布了测试性试验与评价方面的部分规范和工作指南，一定程度上指导了测试性试验与评价工作。但总览技术应用与实践，如何在减少测试性试验风险、成本、周期的同时科学准确地评估测试性水平，实现“快、准、好、省”的测试性试验与评价，仍是需要深入研究的问题。因此，作者在吸收国内外测试性试验与评价技术研究成果的基础上，结合多年来科研、教学和装备型号研制工程经验撰写此书，以全面阐述测试性试验与评价技术内涵、研究现状、工作流程、技术内容及关键技术。书中在总结、阐述测试性试验与评价主要内容、基本流程、经典试验与评价技术的基础上，重点阐述测试性试验方案优化设计技术、等效故障注入方法、测试性指标

综合评估方法、测试性增长试验技术、测试性虚拟试验技术等。

本书在撰写过程中得到了学科带头人温熙森教授的悉心指导。各章作者分别为:第 1 章邱静、刘冠军、张勇,第 2 章张勇、赵志傲,第 3 章张勇、赵志傲,第 4 章邱静、刘冠军、李天梅、王超,第 5 章刘冠军、张勇、李天梅、杨鹏,第 6 章邱静、李天梅、王超,第 7 章吕克洪、赵晨旭,第 8 章张勇、杨鹏、赵晨旭。博士生刘瑛、李华康、季明江、王刚、沈亲沐、谢皓宇、吴超、李乾以及硕士生王贵山、何其彧、林辰龙、方中正、程先哲等参加了全书内容的整理与校对以及部分内容的编撰工作。

本书涉及的相关技术研究与应用得到了军队主管部门、原总装备部通用测试技术专业组和中国航天科技集团公司第一研究院、中国电子科技集团公司第四十一研究所、中国航空工业集团公司第一飞机设计研究院、中国航空研究院 611 所等单位的大力支持,在此深表谢意。空军装备部韩峰岩高工、空军工程大学肖明清教授、湖南大学周志雄教授以及国防科学技术大学胡芎庆教授对本书进行了审阅,并提出了宝贵意见,在此深表感谢。本书的出版得到了科学出版社的大力支持和中国科学院科学出版基金的资助,在此表示衷心的感谢。书中参考和引用了许多国内外有关学者的论文和著作,在此向各位学者表示感谢。

测试性是一门与装备应用结合非常紧密的学科,许多问题尚待进一步研究和探索,特别是将测试性先进理论和技术系统深入地贯彻落实到装备型号研制工程中的路还很长,需要装备管理、论证、设计、研制、试验、使用人员的共同努力。由于作者水平有限,书中难免存在疏漏或不足之处,恳请读者批评指正。

作 者

2016 年 10 月于湖南长沙国防科学技术大学

目　　录

《装备测试性工程系列丛书》序
前言
第 1 章　绪论 …… 1
1.1　测试性试验与评价内涵 …… 1
1.1.1　测试性试验与评价概念及意义 …… 1
1.1.2　装备全寿命周期测试性试验与评价工作内容 …… 1
1.2　基于故障注入的测试性试验与评价流程及关键技术 …… 4
1.2.1　基本流程 …… 4
1.2.2　关键技术 …… 5
1.3　测试性试验与评价现状 …… 6
1.3.1　测试性试验与评价标准方面 …… 6
1.3.2　测试性试验与评价关键技术方面 …… 6
1.3.3　测试性使用评价方面 …… 13
1.4　本书内容安排及所提供的技术支持 …… 14
参考文献 …… 17
第 2 章　测试性试验的数理统计基础 …… 21
2.1　概述 …… 21
2.2　测试性参数 …… 22
2.2.1　故障检测率 …… 23
2.2.2　故障覆盖率 …… 24
2.2.3　故障隔离率 …… 24
2.2.4　虚警率 …… 25
2.2.5　平均故障检测时间 …… 26
2.2.6　平均故障隔离时间 …… 27
2.2.7　BIT/ETE 的可靠性维修性参数 …… 27
2.2.8　测试性指标观测值的随机性 …… 28
2.2.9　测试性预计的局限性 …… 29

2.3 随机变量及其分布 …… 32
2.3.1 基本事件与样本空间 …… 32
2.3.2 大数定律与中心极限定理 …… 32
2.3.3 随机变量 …… 34
2.3.4 测试性试验中常用的分布 …… 34
2.4 经典数理统计理论 …… 36
2.4.1 抽样理论基本概念 …… 37
2.4.2 统计推断 …… 38
2.4.3 测试性试验中的抽样检验理论 …… 44
2.4.4 经典数理统计方法的优缺点 …… 47
2.5 Bayes 统计理论 …… 48
2.5.1 Bayes 统计使用的三类信息 …… 48
2.5.2 Bayes 定理 …… 49
2.5.3 先验分布 …… 49
2.5.4 后验分布 …… 52
2.5.5 Bayes 统计推断 …… 53
2.5.6 Bayes 统计理论的优缺点 …… 54
2.6 本章小结 …… 54
参考文献 …… 54
第 3 章 经典测试性试验方案 …… 56
3.1 概述 …… 56
3.2 测试性试验样本量确定方法 …… 57
3.2.1 基于二项分布的样本量确定方法 …… 57
3.2.2 基于正态近似的样本量确定方法 …… 66
3.3 样本量分配与故障模式抽样 …… 69
3.3.1 按比例的简单随机抽样方法 …… 69
3.3.2 按比例分层分配方法 …… 71
3.4 故障率估计方法 …… 71
3.4.1 基于专家数据的故障率估计方法 …… 72
3.4.2 基于 Bootstrap 方法的故障率极大似然估计及分析 …… 74
3.5 本章小结 …… 77
参考文献 …… 77

第 4 章　测试性试验方案优化设计 …… 79
4.1　概述 …… 79
4.2　经典测试性试验方案问题分析 …… 80
4.3　测试性多源先验数据分析及处理 …… 81
4.3.1　测试性摸底先验数据分析及处理 …… 81
4.3.2　测试性增长试验信息分析及处理 …… 84
4.4　测试性试验方案优化设计 …… 87
4.4.1　基于比例因子的试验方案 …… 87
4.4.2　基于 Bayes 后验风险准则的试验方案 …… 89
4.4.3　基于 SPOT 方法的试验方案 …… 95
4.4.4　基于截尾 SPOT 方法的试验方案 …… 107
4.5　本章小结 …… 114
参考文献 …… 114
第 5 章　测试性试验实施与故障注入 …… 116
5.1　概述 …… 116
5.2　测试性试验准备与实施 …… 116
5.2.1　测试性试验准备 …… 116
5.2.2　测试性试验实施 …… 117
5.3　故障注入基本原理与常用故障注入方法 …… 120
5.3.1　故障注入基本原理 …… 120
5.3.2　故障注入方法分类 …… 120
5.3.3　基于模拟的故障注入方法 …… 121
5.3.4　基于物理的故障注入方法 …… 126
5.3.5　典型的故障注入系统 …… 134
5.4　基于故障传递特性的位置不可访问故障注入方法 …… 136
5.4.1　测试性验证试验故障注入有效性分析 …… 137
5.4.2　故障传递特性分析与量化 …… 143
5.4.3　基于故障传递特性的故障建模 …… 150
5.4.4　基于故障传递特性的位置不可访问故障注入 …… 150
5.4.5　应用案例 …… 152
5.5　本章小结 …… 155
参考文献 …… 155

第 6 章 测试性指标评估方法 …… 157
6.1 概述 …… 157
6.2 经典测试性指标评估方法 …… 158
6.2.1 点估计方法 …… 158
6.2.2 区间估计方法 …… 159
6.2.3 FDR/FIR 估计精度分析 …… 162
6.3 基于多源先验数据的测试性指标评估 …… 167
6.3.1 先验分布及其参数确定 …… 168
6.3.2 多源先验数据相容性检验及可信度计算 …… 175
6.3.3 基于多源先验数据的测试性指标评估模型 …… 178
6.3.4 应用案例 …… 179
6.4 基于 Bayes 变动统计理论的测试性指标评估 …… 184
6.4.1 总体技术思路 …… 184
6.4.2 FDR/FIR 的 Bayes 评估模型 …… 185
6.4.3 模型稳健性分析 …… 196
6.4.4 验证评估案例 …… 198
6.5 本章小结 …… 206
参考文献 …… 207
第 7 章 测试性增长试验技术 …… 208
7.1 概述 …… 208
7.2 测试性增长的概念与途径 …… 209
7.2.1 测试性增长的基本概念 …… 209
7.2.2 测试性增长的时效性 …… 210
7.3 测试性增长试验的概念与流程 …… 213
7.3.1 测试性增长试验的概念 …… 213
7.3.2 测试性增长试验的流程 …… 214
7.4 测试性增长试验的规划研究 …… 217
7.4.1 基于及时纠正的试验规划研究 …… 217
7.4.2 基于延缓纠正的试验规划研究 …… 223
7.5 测试性增长试验的跟踪预计研究 …… 227
7.5.1 基于 Bayes 统计理论的测试性增长指标评估 …… 227
7.5.2 考虑非理想纠正的增长概率模型 …… 230

7.5.3　测试性增长跟踪预计曲线绘制 …… 237
7.6　本章小结 …… 239
参考文献 …… 239
第 8 章　测试性虚拟试验技术 …… 242
8.1　概述 …… 242
8.2　测试性虚拟试验的基本流程 …… 243
8.3　测试性虚拟试验的关键技术 …… 243
8.3.1　面向测试性的虚拟样机建模技术 …… 243
8.3.2　基于模型的故障注入样本序列生成技术 …… 270
8.4　测试性虚拟试验案例 …… 296
8.4.1　导弹控制系统 …… 297
8.4.2　航向姿态系统 …… 317
8.5　基于实物试验与虚拟试验相结合的测试性试验技术 …… 330
8.6　本章小结 …… 332
参考文献 …… 332
附录 A　标准正态分布表 …… 334
附录 B　*t* 分布表 …… 335
附录 C　*F* 分布表 …… 338
附录 D　二项分布单侧置信下限 …… 350
附录 E　二项分布单侧置信上限 …… 354

第 1 章　绪　　论

1.1　测试性试验与评价内涵

1.1.1　测试性试验与评价概念及意义

测试性是指装备能及时准确地确定其状态(可工作、不可工作或性能下降),并有效隔离其内部故障的一种设计特性[1,2]。良好的测试性设计对于提高装备的维修保障水平和战备完好性、降低全寿命周期费用等具有重要意义[3,4]。

近年来,测试性作为装备的一个重要特性越来越受到重视,订购方对飞机、导弹、雷达等新型装备提出了明确的测试性指标要求。随着装备测试性工程的推进,如何发现测试性设计不足、指导测试性改进,如何判断装备的测试性指标是否达到合同规定的要求,如何给出订购方和承制方都认可的合理评价,成为装备面临的现实问题,也正是开展测试性试验与评价工作的意义所在[5,6]。

广义上,检验或评价产品测试性水平的工作都可以纳入测试性试验与评价的范畴。GJB 3385—98《测试与诊断术语》描述的测试性验证是测试性试验与评价中的关键工作之一,其定义为:为检验研制产品满足合同规定的测试性要求而进行的工作[7]。测试性试验与评价的目的有:①识别装备的测试性设计缺陷,采取有效的措施予以纠正,实现测试性的持续改进和增长;②承制方对装备的故障检测率、故障隔离率等测试性水平进行摸底,判断装备当前测试性水平与合同规定的设计要求之间的差距;③订购方评估、确认装备的测试性设计水平是否符合规定的测试性定量和定性要求,为装备定型、鉴定或验收提供依据;④评估、确认装备在实际使用中的测试性水平,为测试性熟化、改进测试性水平提供指导。测试性试验与评价工作直接影响装备的研制质量和进度,是保证和检验装备测试性水平的重要环节。

1.1.2　装备全寿命周期测试性试验与评价工作内容

国内外相关标准和文献对测试性试验与评价的内容划分描述不一。按全寿命周期内工作时机和目的,测试性试验与评估内容可分为研制阶段的测试性核查、定型与验收阶段的测试性验证以及实际使用阶段的测试性使用评价。

装备全寿命周期内测试性试验与评价工作流程如图 1.1 所示。

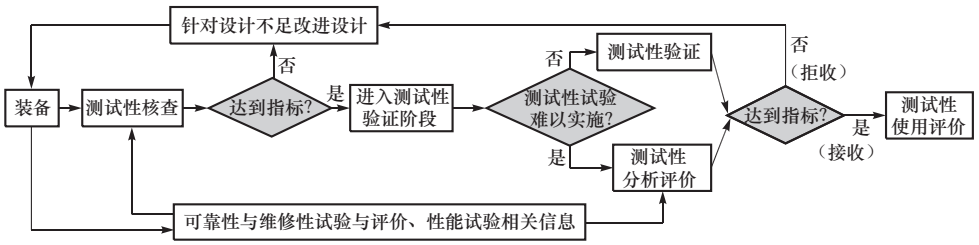

图 1.1 全寿命周期内测试性试验与评价工作流程

1）测试性核查

测试性核查是承制方为实现装备的测试性要求，贯穿于整个设计研制过程的试验与评价工作。测试性核查的主要目的是对各种研制试验过程中的故障检测、隔离结果及虚警情况进行分析和评价，发现测试性设计缺陷并采取改进措施，使装备测试性得到持续改进。

测试性核查主要包括测试性分析与预计、固有测试性核查、测试性研制试验等[8,9]。测试性分析与预计一般是在方案阶段进行测试性建模与分析，估计装备可达到的测试性水平，为选择设计方案或转入新的研制阶段提供依据，目前可采用的测试性建模与分析工具包括 TEAMS、eXpress、TADES 等[4,10-12]。固有测试性核查有助于识别固有测试性设计的缺陷，确保固有测试性设计的有效性。测试性研制试验一般是在产品样机研制出后，为确认产品的测试性设计特性和暴露产品的测试性设计缺陷，由承制方或指定的试验机构，在产品的半实物模型/样机/试验件上开展的故障注入/模拟试验与分析过程。测试性摸底试验是指为在定型阶段的装备测试性验证前做到“心中有数”，全面检查产品测试性设计效果的一种测试性研制试验。测试性分析与预计、测试性研制试验等是测试性增长的重要过程[13,14]。

2）测试性验证

测试性验证是指由订购方指定的试验机构在实验室或实际使用环境下，按抽样设计的试验方案，对装备实物样机注入一定数量的故障，用测试性设计规定的方法进行故障检测与隔离，评估装备的测试性水平，判断是否达到规定的测试性定量要求。测试性验证一般在定型阶段进行。“测试性验证”术语来源于 GJB 3385—98《测试与诊断术语》和 GJB 2547—95《装备测试性大纲》[7,15]。在 GJB 2547A—2012《装备测试性工作通用要求》中，将“测试性验证”改称为“测试性验证试验”，但工作内容基本没变[2]。考虑到测试性验证的工作内容既包括试验又包括评价，“测试性验证试验”术语不便于涵盖所有验证工作，本书在此沿用 GJB 3385—98《测试与诊断术语》和 GJB 2547—95《装备测试性大纲》中的术语，还是称为“测试性验证”，而将测试性验证中开展的试验称为“测试性验证试验”。

测试性验证包括为装备设计定型提供依据而进行的测试性鉴定和为验收批量

装备的测试性水平而进行的测试性验收。对于难以实施测试性验证的产品，可收集产品与测试性有关的设计资料、试验数据、运行数据等，通过工程分析、虚拟样机建模分析等途径进行综合分析，评价装备是否满足规定的测试性要求，即以综合分析评定代替测试性验证来确定是否符合规定的测试性要求，为装备设计定型提供依据。这种手段在GJB 2547A—2012《装备测试性工作通用要求》中称为“测试性分析评价”。近年来，基于虚拟样机的测试性虚拟试验得到了一定程度的研究与发展，可作为测试性分析评价的一种有效手段[16-19]。

测试性验证是订购方主导、承制方参与，一般委托第三方评价机构进行的测试性试验与评价活动，主要服务于装备的设计定型，验证结果是装备设计定型的重要依据。其规程与质量体系要求严格，技术与实施过程规范，是装备测试性试验与评价中的关键工作，也是具有技术代表性的测试性试验与评价工作。

3）测试性使用评价

测试性使用评价是指在实际使用条件下，为评价装备的实际测试性水平而进行的工作。其主要目的是评价装备在实际使用条件下达到的测试性水平，确定是否满足规定的测试性要求，发现装备的测试性缺陷，为外部测试设备的改进、装备改型和新装备研制等提供支持信息。装备部署后，通过收集装备在实际使用中的测试性数据，获得足够的数据量后，用选定的统计分析方法（如区间估计、点估计等）确认装备的测试性水平，评价其是否满足规定的要求。此阶段不再采取故障注入试验，而是让装备自然发生故障并实施故障检测/隔离，所收集到的测试性数据是最可信的，评估结果也最接近真实值，但需要很长的时间。

4）各项测试性试验与评价工作对比与联系

从试验阶段、试验目的、试验方式、试验场所、实施者等方面进行对比，各项测试性试验与评价工作对比情况见表1.1。

表1.1 各项测试性试验与评价工作对比

类型	试验阶段	试验目的	试验方式及内容	受试品	试验场所	优缺点	实施者
测试性核查	研制阶段	暴露测试性设计缺陷、改进测试性、测试性增长、测试性摸底	测试性分析与预计、固有测试性核查	设计方案、图纸	实验室	代价小，准确性低	承制方或委托第三方评价机构
			测试性研制试验：以故障注入为基本手段的试验	实物样机	实验室	准确性高，代价大	
测试性验证	定型、验收阶段	确定装备的测试性指标是否满足合同规定的要求	测试性验证试验：以故障注入为基本手段的试验为主，必要时辅以测试性分析评价	实物样机为主，虚拟样机为辅	实验室为主	订购方采信的主要方式，代价大，准确性高	订购方主导，委托第三方评价机构
测试性使用评价	使用阶段	确定装备的测试性水平是否满足规定的使用要求	收集装备在使用中的测试性数据，评价装备测试性水平	实物装备	使用现场	准确性高，数据收集时间长	使用单位或第三方评价机构

上述工作既有区别，又相互联系。测试性核查主要是在装备研制阶段通过试验和分析等方式检查测试性设计工作的有效性，纠正设计缺陷，实现测试性增长，逐步达到测试性的各项要求，为确保测试性验证顺利通过奠定基础。测试性核查信息可为测试性验证提供支持；测试性验证的结果可以为检验测试性核查工作的正确性提供依据和参考。测试性核查报告中的各种有关数据还是测试性验证阶段测试性分析评价所收集数据的重要组成部分，测试性核查和测试性验证的最终目的是确保投入使用的装备测试性满足要求。测试性使用评价结果可用于检验测试性核查和测试性验证工作的正确性，也可用于指导使用期间测试性改进。

测试性验证是要求规范、具有技术代表性的测试性试验与评价工作，对试验方案的确定、试验实施与故障注入方式、指标评估方法都有规范、严格的规定。测试性核查中的测试性研制试验方案制定比较灵活，既可以采用规范、确定的试验方案，也可根据设计要求、测试性工作计划和具体评价项目需求等确定，故障注入方式与验证中的故障注入试验基本相同。测试性使用评价中主要是收集装备使用阶段发生的故障及测试信息进行评价。测试性核查、测试性验证、测试性使用评价三者的指标评估方法都是基于概率统计理论，但其数据来源不同。

可以看出，上述工作在技术上存在一定的共性。其中，在实物装备上注入故障为基本手段进行的测试性试验与评价是现阶段典型的试验与评价方式，主要包括研制阶段的测试性研制试验与评价、定型验收阶段的测试性验证等。如何准确、高效地进行该方面的工作综合反映了测试性试验与评价中的共性关键技术问题，如试验方案的科学合理设计、故障注入、指标评估等。该方面技术的研究，对于装备测试性研制试验与评价、测试性增长、测试性摸底、测试性验证及测试性使用评价都具有重要意义。本书即主要围绕其基本过程与关键技术进行阐述，测试性试验与评价中的其他内容如固有测试性核查等，可参考 GJB 2547A—2012《装备测试性工作通用要求》[2]，基于模型的测试性分析与预计技术可参考本套《装备测试性工程系列丛书》之二——《装备测试性建模与设计技术》等[4]。

1.2 基于故障注入的测试性试验与评价流程及关键技术

1.2.1 基本流程

在实物装备上注入故障为基本手段进行的测试性试验与评价基本流程如图 1.2 所示，主要包括试验组织建立、产品技术状态确认、产品故障模式及影响分析确认、测试性试验大纲制定与评审、试验方案设计与试验前检查、测试性试验实施、测试性试验报告编写与评审等环节。其中，试验组织建立、产品技术状态确认是进行测试性试验的前提，产品故障模式及影响分析确认是测试性试验与评价的

主要输入，而测试性试验方案设计、测试性试验实施是测试性试验与评价的关键技术环节。

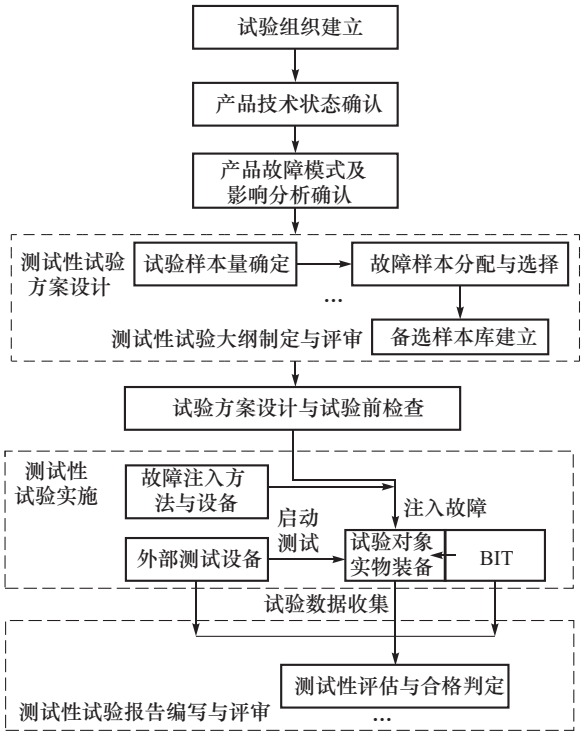

图1.2　实物装备注入故障为基本手段的测试性试验与评价流程

1.2.2　关键技术

1）测试性试验方案设计

测试性试验方案又称抽样方案，承制方和订购方在考虑测试性指标要求、双方试验风险、试验成本等多种因素的基础上，基于统计理论等计算或选择测试性试验方案，主要包括：注入多少故障，注入哪些故障。测试性试验方案用于指导测试性试验的实施和测试性水平的评价，其关键之处在于要选择出与装备故障实际发生规律尽量一致、样本量尽量较少、满足统计评估准确性要求的故障样本集，其合理性直接影响测试性试验的可行性、试验代价、测试性评估结论的准确性等[20-24]。因此，测试性试验方案设计是测试性试验与评估的关键技术之一。

2）测试性试验实施

测试性试验实施的基本过程为：①根据试验方案确定待注入的故障样本，采用合适的故障注入方法与设备，向受试装备注入故障；②装备开机，启动装备测试性

设计所配置的机内测试、外部测试设备等对所注入的故障进行故障检测与隔离；③记录检测与隔离结果。该过程中，由于故障注入可能给装备带来破坏，而且有些位置不允许进行注入，故障注入问题成为测试性试验实施中的瓶颈，故障注入技术是需要研究的关键技术之一[20,25,26]。

3）测试性评估

测试性评估是分析测试性试验数据，判定装备的测试性水平是否达到规定的要求，发现测试性设计问题，给出测试性改进建议。测试性评估可以得出装备的测试性指标点估计值或区间估计值，并可以此为依据给出是否接收的判定参考。如果试验方案不够合理，或者需要注入的故障难以注入，会因试验数据不充分影响评估准确性。如何提高测试性评估准确性和可信性是需要解决的关键问题之一。

1.3 测试性试验与评价现状

1.3.1 测试性试验与评价标准方面

美军标 MIL-STD-471A[27] 及其 1978 年颁布的通告 2 *Demonstration and Evaluation of Equipments/System Built-in Test/External Test/Fault Isolation/Testability Attributes and Requirements*[28] 是最早以军用标准形式规定了实际装备测试性试验细则。类似的规范性文件还包括美国 AD-A081128 报告 *BIT/External Test Figures of Merit and Demonstration Techniques*[29]、MIL-STD-2165 *Military Standard Testability Program for Electronic Systems and Equipments*[1] 等。英国颁布的 Def Std 00-43(Part 2)/Issue 1 *Reliability and Maintainability Assurance Activity Part 2:Maintainability Demonstrations*[30] 更是要求测试性试验完全按照 MIL-STD-471A 的方法执行。2012 年，我国在国军标 GJB 2547—95《装备测试性大纲》的基础上，修订并颁布了 GJB 2547A—2012《装备测试性工作通用要求》[2]，简要阐述了测试性试验的目的、要求等，是开展测试性试验的牵头性标准，对测试性试验给出了规范性指导。

1.3.2 测试性试验与评价关键技术方面

测试性分析与预计等技术现状在其他文献中已有较多总结，这里针对基于故障注入的测试性试验与评价的关键技术进行总结与分析。

1. 测试性试验方案设计技术

测试性验证中的试验方案主要包括确定故障样本量、故障模式抽取、接收/拒

收判定等，如图1.3所示。

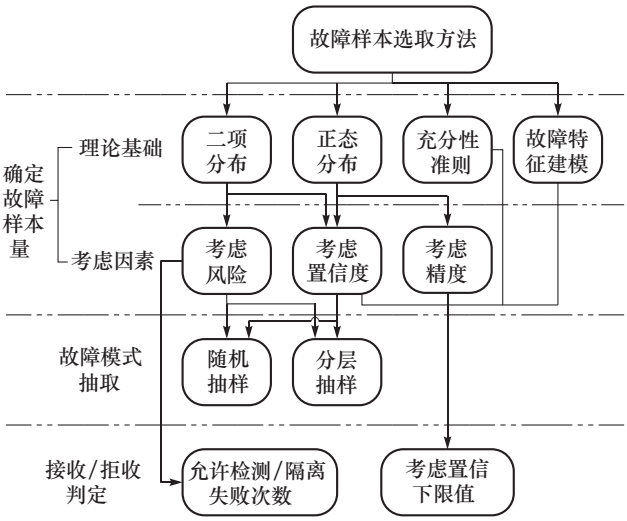

图1.3 试验方案设计基本流程及方法分类

GJB 2547A—2012规定承制方应根据有关标准和资料(如GJB 2072—94的附录C等)确定测试性试验方案，并经订购方同意，也可以使用由订购方提供的并经承制方认可的其他试验方案。测试性验证试验采用统计试验的方法，常见的确定故障样本量的统计检验模型有二项分布模型和正态分布模型。在相同的检验模型下，确定故障样本量一般有两种原则：一是考虑试验费用、承制方风险和订购方风险确定故障样本量；二是考虑装备测试性指标评估的精度或置信度确定故障样本量。

1) 基于二项分布的试验方案设计方法

基于二项分布的故障样本选取方法是将故障检测/隔离试验看作成败型试验，利用二项分布抽样特性函数，考虑FDR/FIR的指标要求值、FDR/FIR最低可接收值、承制方风险和订购方风险，确定故障样本量和允许的检测/隔离失败次数，即抽样方案。若只考虑订购方风险，确定的抽样方案称为极限质量(limit quality，LQ)抽样方案。同理，也可只考虑承制方风险制定抽样方案。基于这一思想进行试验方案设计的文献有：GJBz 20455—97《地面无线电引信对抗设备试验场试验方法》[31]、GJB 1298—91《通用雷达、指挥仪维修性评审与试验方法》[32]、GB 5080.5—85《设备可靠性试验 成功率的验证试验方案》[33]等。AD-A081128报告*BIT/External Test Figures of Merit and Demonstration Techniques*[29]也是基于二项分布假设，考虑FDR/FIR的指标要求值、FDR/FIR最低可接收值、承制方风险和订购方风险，利用二项分布与正态分布的近似关系，确定抽样方案。在试验结

束后以故障检测/隔离失败次数作为接收/拒收判据。还有一种基于二项分布确定故障样本量的方法是考虑 FDR/FIR 的最低可接收值和相应估计值的置信度，利用二项分布抽样特性函数，求得达到 FDR/FIR 的最低置信下限值需要的故障样本量，对于 FDR/FIR 要求高的装备，允许的故障检测/隔离失败次数为 0，基于此可以求得最少故障样本量。

2) 基于正态分布的试验方案设计方法

基于正态分布的故障样本选取方法是一种统计评估方法，考虑的因素为 FDR/FIR 估计的精度或置信度，理论基础是伯努利大数定律和中心极限定理，即当故障样本量足够大时，二项分布可以用正态分布来近似，且 FDR/FIR 估计值的偏差近似服从正态分布。MIL-STD-471A *Maintainbility Verification/Demonstration/Evaluation* 及其 1978 年颁布的通告 2 *Demonstration and Evaluation of Equipments/System Built-in Test/External Test/Fault Isolation/Testability Attributes and Requirements*[27,28] 是最早以军用标准形式规定的较完整的用于指导实际装备测试性验证试验故障样本选取的方法。该方法是以简单的正态分布区间估计公式为基础计算 FDR/FIR 估计值的上限值和下限值及接收/拒收判据。试验后采用正态分布置信限公式进行 FDR/FIR 的接收/拒收判断。1995 年，MIL-STD-471A 改版为 MIL-HDBK-471 *Maintainbility Verification/Demonstration/Evaluation*，但对上述内容未作进一步的修订。GJB 1135.3—91《地空导弹武器系统维修性评审、试验与评定》[34] 给出了基于正态分布假设的地空导弹武器系统 BIT 和外部检测设备的 FDR/FIR 验证的故障样本量确定方法。该方法以简单的正态分布分位点估计和 FDR/FIR 估计值的允许偏差为基础计算故障样本量及接收/拒收判据。在确定故障样本量后，不需要进行故障样本量分配，直接从被测单元(unit under test，UUT)故障模式集中随机抽取故障模式构成故障样本集。GJB 1770.3—93《对空情报雷达维修性　维修性的试验与评定》[35] 给出了基于正态分布假设的对空情报雷达 BIT 的 FDR/FIR 验证的抽样方案确定方法。该标准依然采用 GJB 1135.3—91 方法计算故障样本量，但将 GJB 1135.3—91 方法中的分位点值修正为一定的置信水平值。研究表明，以正态分布为基础的方法是近似方法，误差比较大，特别是对于 FDR/FIR 的指标大于 0.9 的情况。

此外，国内外还研究了其他测试性试验方案设计方法，如基于充分性度量准则的故障样本确定方法[9]、基于故障特征模型的故障样本确定方法等，这些方法在测试性研制试验等方面也具有一定的应用价值。

在确定了故障样本量的基础上，需要从 UUT 故障模式集中抽取规定数量的故障模式构成故障样本集。一种方法是根据 UUT 各组成单元的故障率(基于可靠性预计结果)大小进行故障样本量的分配，确定每个组成单元要注入的故障模式数量，并从组成单元的故障模式集中随机抽出规定数量的故障模式，即分层抽样

的方法[36]。另一种方法是直接从 UUT 故障模式集中随机抽取故障模式构成故障样本集，即随机抽样的方法[36]。

接收/拒收判据和故障样本量确定基于同一理论：一种是基于二项分布确定的抽样方案进行接收/拒收判定，另一种是根据试验评估结果给出 FDR/FIR 的置信下限值，并与规定的最低可接收值进行比较，给出接收/拒收判定结论。

表 1.2 给出了目前常用的三种试验方案及其特点与适用条件[2,9]，其中 α 为承制方风险，β 为订购方风险。

表 1.2 常用测试性试验方案

试验方案	主要特点	适用条件
最低可接收值试验方案(基于二项分布和检验充分性)	合格判据合理、准确；考虑产品组成特点；可查数据表，方法简单；可给出参数估计值	适用于验证指标的最低值；不适用于有 β 要求的情况
考虑双方风险的试验方案(基于二项分布)	合格判据合理、准确；可查数据表，相对简单；未给出参数估计值；未考虑产品组成特点	要求首先确定鉴别比和 α、β 的量值；不适用于有置信度要求的情况
GJB 2072—94 的试验方案(基于正态分布的试验方案)	比 MIL-STD-471A 通告 2 方法有改进；可计算出下限值近似值；准确度较低；未考虑产品组成特点	适用于验证指标的最低值；不适用于有 α、β 要求的情况

当对装备的测试性指标要求较高，承制方、订购方最大风险承受能力低，或者要求的评估结论置信度、精度较高时，按已有方法确定的故障样本量通常很大。往往存在一些危害性极大且不允许注入的故障和不能有效注入的故障，导致故障样本结构不合理等问题[20,23,37,38]。

针对故障样本量大、故障样本结构不合理等问题，需对试验方案开展优化设计技术研究，合理减少故障样本量、优化抽样方案、优化故障样本结构。

2. 故障注入技术

故障注入的实施是测试性试验中的一项关键环节，能否安全有效地注入故障样本决定着试验的成败。故障注入可由硬件、软件或软硬件共同实现。下面简要介绍国外总结的常见故障注入实现方法。

1) 模拟故障注入

模拟故障注入方法是指在系统的仿真模型中插入故障注入单元来实现故障注入[39,40]。这种方法通常应用于设计周期的前期阶段，即系统物理样机建立之前。模拟故障注入工具一般采用 VHDL 生成，也有的工具在现有模拟模型基础上加入故障注入功能构成。模拟故障注入方法虽然具有费用低廉、不需要任何特殊的硬件、对注入的故障可以精确地监控、注入故障模式多等优点，但其缺点也很明显，如在没有有效的仿真器的情况下开发工作量大，建立详细精准的仿真

模型一般非常困难导致仿真模型置信度低，不能捕获系统的真实行为，也不能说明真实系统的执行错误。考虑到基于模拟的故障注入方法的上述优缺点，在装备研制初期，在没有物理样机时，可以采用该方法作为开展测试性试验的有效手段。模拟实现的故障注入工具的典型代表有德国 Erlangen-Nürnberg 大学开发的 VERIFY[41]、瑞典 Chalmers 技术大学开发的 MEFISTO-C[42]、美国 Illinois 大学开发的 FOCUS 等[43,44]。

2）硬件故障注入

硬件故障注入主要是通过宿主机控制注入故障的类型及注入故障的时间，使用硬件设备进行故障注入，并收集系统在注入故障后的响应及测试结果。引入的错误类似于芯片内部失效引起的错误以及由环境干扰引起的错误。该方法注入的故障更接近于系统运行现场中可能发生的真实硬件故障，注入故障位置、范围广，故障传播性好。随着故障注入应用范围的不断扩大和评测的目标系统结构复杂性的不断提高，硬件故障注入方法的局限性逐渐暴露出来[45]。例如，硬件故障注入需直接将硬件插入到目标系统中，容易对硬件造成损坏，且价格昂贵，可控性差，被测对象硬件结构的复杂性使得故障注入后的测试变得困难。因此，硬件故障注入大多应用在设计阶段，产品完成后的验收阶段不可能再开箱分解测试，导致许多硬件故障注入无法进行，且硬件故障注入无法评测软件故障情况。国外针对电子系统的知名硬件注入系统主要有瑞典 Chalmers 技术大学开发的 FIST[46]、法国 LASS-CNRS 大学开发的管脚级故障注入工具 Messaline[47]、奥地利 Vienna 技术大学开发的 MARS[45]等。

3）软件故障注入

软件故障注入[48]提供了廉价和易于控制的故障注入方法。软件故障注入无需额外的硬件设备，可以在程序指令能够访问到的硬件或软件上选择故障注入的位置。许多软件故障注入可以用来模拟硬件故障，故障可能出现在 CPU、内存、总线或网络上，这些故障会导致软件执行错误，如执行不正确的指令或访问不正确的数据。软件故障注入主要通过修改内存或寄存器的值来实现。但由于系统及软件本身的复杂性和多样性，在实现上有很多不同方法，如基于调试器的故障注入方法、基于驱动的故障注入方法、基于特定目标系统的故障注入方法及基于多处理器的故障注入方法[49]。软件故障注入方法的优势之一就是完成故障注入相对经济，因为它不需要特定的硬件或仿真器，相对于硬件故障注入，它可以注入指定的故障，并可以多次重复注入。但是，软件故障注入通常是通过修改目标程序语句，需要在目标程序中插入特定程序代码，属于侵入性故障注入，尤其对强实时嵌入式系统和内存资源紧张的系统，软件故障注入方式甚至会严重地影响系统的性能。虽然软件注入可以注入许多硬件不能注入的故障，如寄存器崩溃故障，但通过软件完成的故障注入只能限制在和软件有关的部分，如软件注入不能使 CPU 在系统总线