基于故障注入的雷达软件安全性测试

赵国利[1] 敬 敏[2]
ZHAO Guoli JING Min

摘 要 雷达软件的安全性是装备安全的重要内容，软件测试是提高雷达软件安全性的重要方法。从遇到的历史典型问题入手，利用故障模式及其影响危害性分析（FMECA）技术分析历史故障对系统安全性产生的影响，找出典型故障模式并设计测试用例，然后使用故障注入技术进行安全性测试，并结合某典型雷达系统开展实例验证研究。结果表明，基于故障注入的雷达软件安全性测试技术可有效提升雷达软件安全性测试能力，提升雷达系统发现系统故障和问题的能力，降低系统运行故障率，提高雷达软件安全可靠性水平。

关键词 软件安全性；故障注入；故障模式；软件测试；雷达软件

doi：10.3969/j.issn.1672-9528.2024.09.042

0 引言

随着雷达系统的日益复杂，软件在雷达产品中完成功能的比例和重要性日益上升，成为影响系统安全性的关键因素。雷达系统运行过程中会出现各类故障，导致软件失效，可能带来灾难性的后果或重大经济损失，成为雷达系统质量提升的瓶颈所在。

软件安全性是指软件运行不引起危险和灾难的能力，除保证系统正常运转而必须工作的功能之外，软件安全性重点关注系统正确运行的情况下不应出现的系统危险，可能导致某个危险的情况或者其他不期望的结果。软件安全性更加关注那些引起灾难性事故发生的失效，是为了避免灾难性事故的发生[1]。因此，软件安全性测试的目标就是通过测试发现软件中存在的缺陷，并进行修正，以快速降低由于软件失效而导致系统事故的风险[2]。所以，如果能够分析出系统的危险所在，并加强对这些部分的测试，既可以最大程度地保持系统的安全性，又可以整体提高测试的效率。

软件安全性测试是雷达装备软件测试中常见的测试类型，常用的方法有故障树分析测试法、猜错测试法等，其依据通常基于软件需求。例如，叶婷等人[3]使用面向需求的软件安全性测试方法，对软件安全性测试用户需求进行了分类讨论，并对相应的软件安全性测试方法进行逐一阐述；张风玲等人[4]从安全性需求来源、安全性测试要点的角度，对嵌入式软件的安全性测试进行了研究，从专用和通用安全性需求的角度，开展有状态明确安全性、关键数据处理安全性、运算安全性、通信安全性、终端资源安全性等安全性测试；赵昶宇[5]提出了一种嵌入式软件安全性测试的方法，利用统计测试功能剖面生成的方法提取重要功能集合生成软件安全性测试剖面，进而设计测试用例开展软件安全性测试；李震等人[6]运用故障树模型的最小割集思想分析了导致安全问题各个因素，生成最小割集，设计测试用例开展安全性测试，保障测试充分性和合理性；董燕等人[7]提出一种基于软件故障注入的安全性测试方法，通过构建全数字仿真测试环境，模拟目标系统输入异常故障及运行态异常故障，可以灵活地实现软件故障注入。

然而，上述软件测试方法中，使用可靠性测试的方法来开展软件安全性测试，或者主要基于需求已定义的边界或异常等例外情况来开展测试，而忽略已发生的历史故障对软件安全性的潜在影响。故障注入方法可加速系统故障进程，关注历史故障对系统安全性的影响，但传统的故障注入方法侧重仿真环境的搭建和使用，缺少对软件安全性关联故障来源和故障模式的分析，影响软件测试问题检出效率，导致其在雷达领域应用较少。

针对上述问题，本文提出了基于故障注入的雷达软件安全性测试方法，通过故障模式及其影响危害性分析（FMECA）技术对各模块发生故障对系统安全性的影响进行分析，找出典型故障模式，然后对其设计测试用例使用故障注入技术进行安全性测试。本文研究成果可以提升雷达系统发现系统故障和问题的能力，降低系统运行故障率，提高雷达软件安全可靠性水平。

1. 南京电子技术研究所 江苏南京 210039
2. 解放军 93145 部队 江苏南京 210039

1 典型雷达系统故障模式识别与分析

1.1 雷达系统故障模式的识别方法

为提高雷达软件和系统的安全性，根据历史雷达系统故障数据，充分识别雷达系统典型故障模式，为提升软件安全性测试验证的有效性与可行性奠定输入基础。依据 GJB 451A-2005 中的描述，故障模式是故障的表现形式。更确切地说，雷达系统故障模式是对雷达产品所发生的、能被观察或测量到的故障现象的规范描述。

识别雷达系统故障模式的途径主要有以下两种。

（1）基于历史数据的故障模式识别：依据雷达系统历史故障数据，借助模式识别、一阶谓词、集合论等技术，从中挖掘“雷达系统设计要素”“雷达系统异常行为”等知识，形成雷达软件专用故障模式。这种故障模式识别方法的主要优点在于，历史故障数据中蕴含丰富的雷达系统失效经验，也是新系统研发和使用过程中最容易出现的问题。收集历史软硬件故障数据，分析形成典型雷达系统故障模式，可以快速识别雷达系统设计薄弱环节，并有效避免类似雷达系统问题的重复发生。

（2）基于标准要求的故障模式识别：通过调研 GJB/Z 102A、GJB/Z 142、GJB 2547A 等相关标准以及其他类似系统中的故障模式，选择形成适用于雷达系统的故障模式。这种故障模式识别方法的优点在于，可以让标准要求和类似工程经验在雷达系统设计中落地，从而确保雷达系统研制过程的规范性和有效性。

1.2 典型雷达系统故障模式及其分类

依据上述雷达系统故障模式识别方法，对典型历史雷达系统故障数据进行总结与分析，并进行故障影响及危害性分析，形成典型雷达系统故障模式，应用于雷达软件安全性测试。

分析故障模式对系统使用、功能或状态产生的影响，并根据最终影响确定严酷度等级，得到故障影响及危害性分析结果。根据分析结果形成需进行安全性测试的典型雷达系统故障模式。针对典型雷达系统故障模式，主要从软件处理角度进行分类。

输入故障相关的故障模式，即错误输入数据或指令导致的故障，如界面和接口输入、文件输入、鼠标操作、输入顺序、接口组合等。

输出故障相关的故障模式，即软件错误的输出故障，典型如输出数据未遵守接口协议规范、无激励信号输出、输出数据不完全或遗漏、输出数据变化幅度过大或速度较快等。

程序处理故障相关的故障模式，即执行资源、过程、错误处理等程序处理过程导致的故障，典型如中断、接口、时钟等资源使用不当，程序初始化（网络、参数、配置、硬件等）失败，未进行跨时钟域处理导致控制失效。

典型雷达系统故障模式的示例和分类如表 1 所示。

表 1 典型雷达系统故障模式及其分类

编号	故障模式	故障模式分类	故障模式来源
FMECA-01	不同模块初始化时间不一致，导致数据阻塞、通信中断	程序处理故障	FRACAS 数据
FMECA-02	总线数据流量超过总线性能指标要求，导致数据阻塞	输入故障	FRACAS 数据
FMECA-03	多线程数据访问冲突，导致系统死机	程序处理故障	FRACAS 数据
FMECA-04	关键开关量信号跳变，导致系统下电	输入故障	FRACAS 数据
FMECA-05	软件从外部存储中读取内容错误的数据，导致系统无法识别	输入故障	FRACAS 数据
FMECA-09	电源模块输出超压，导致天线无法扫描	输出故障	FRACAS 数据
……	……	……	……

2 基于故障注入的雷达软件安全性测试

根据系统故障模式分析结果，选择相应的安全性测试方法开展验证。通过软件、硬件、总线、软硬件结合等手段，将各类故障模式注入系统，设计测试用例触发故障模式，查看故障模式是否被有效控制。

2.1 软件故障注入

软件故障注入是通过在系统 / 设备内、外部软件中注入故障代码或故障行为的一种故障注入方式，这种注入方式较硬件故障注入方式能够对复杂系统行为层面进行故障注入[8]。软件故障注入的主要实施方法为程序变异[9]，即通过直接在软件内插入故障代码，然后将插入故障代码的软件编译下载到目标设备中实施故障注入，根据故障激活的条件又分为编译期故障注入（无条件激活）和运行中故障注入（运行时由外部条件激活）[10-11]。常用的程序变异策略包括边界值法、赋值异变、条件异变等。程序变异的基本原则是变异代码尽可能小地对系统改动，变异影响尽可能大地覆盖系统功能。程序异变的内容包括目标芯片资源故障、总线数据发送故障、系统内部资源故障、系统内部自检测电路故障等。

（1）构建软件故障注入环境

搭建软件故障注入环境，环境中包括故障注入计算机、编译环境、下载或调试仿真设备，在运行程序源码中注入故障代码并编译运行，触发故障条件时，注入的故障将被激活。

（2）基于软件故障注入的测试设计

依据系统故障模式中的故障原因分析，设计测试用例中的软件激励条件，验证系统能够对典型故障模式正确处理。

软件故障注入测试用例要素包含以下内容：名称和标识、测试追踪、用例说明、测试的初始化要求、测试输入、预期输出、评估测试结果的标准、前提和约束等。其中，测试追踪是对被测故障模式的追踪。

（3）基于软件故障注入的测试方法

软件故障注入测试采用黑盒测试方法，包括功能分解、等价类划分、边界值分析、猜错法等。在验证过程中分析故障的特性，采用适当的测试方法进行测试设计。

（4）测试用例及执行结果样例

针对“多线程数据访问冲突，导致系统死机”故障模式，使用软件故障注入方法设计测试用例开展测试，示例见表2。

表2 线程访问冲突防护处理测试用例

测试用例标识	GZZR-003	故障注入方法	软件故障注入
测试用例名称	线程访问冲突防护处理	测试方法	等价类划分
测试追踪	FMECA-03		
测试说明	针对增加线程锁进行保护，当对数据对象进行访问、插入、删除、修改操作时，增加信号量保护，避免直接进行多线程操作。		
测试过程			
序号	输入步骤	预期结果	实际结果
1	在程序中修改多线程数据访问，出现数据读写冲突，运行软件至线程冲突代码处。	软件或系统弹出错误提示，并退出。	软件或系统弹出错误提示，并退出。
2	在程序中增加对该多线程数据访问的限制及保护。运行软件至线程冲突代码处。	软件或系统未出现错误提示或退出崩溃等情况。	软件或系统未出现错误提示或退出崩溃等情况。
通过准则	实际结果与预期结果一致	执行结果	通过

2.2 硬件故障注入

硬件故障注入是在物理层级完成的，通过对电路或相关芯片管脚等施加电源干扰，如电源故障、电压超出有效、过流、极值、斜率等不同，达到故障注入的效果[12-13]。硬件故障注入方法需要专门的硬件设备，实际模拟真实的故障信号，重构故障，并可以详细地分析故障注入对被注入元件的影响。

（1）构建硬件故障注入环境

硬件故障注入环境主要包括硬件故障注入器、模拟电路或芯片正常运行的电源、信号源、示波器等设备。

（2）基于硬件故障注入的测试设计

依据系统故障模式中的故障原因分析，设计测试用例中的硬件激励条件，验证系统能够对典型故障模式正确处理。硬件故障注入测试用例要素与软件故障注入测试用例要素一致。

（3）基于硬件故障注入的测试方法

硬件故障注入的主要方法是电源干扰法，它有两种实现方式：其一是通过硬件故障注入设备产生电压附着于硬件注入点的探针改变经过这些注入点的电流，从而向计算机系统中引入故障；其二是通过硬件故障注入设备完全模拟电路或芯片的运行环境，再改变信号源或故障信号。硬件故障注入形式包含过压、过流、极值、斜率故障等[14]。

（4）测试用例及执行结果样例

针对“关键开关量信号跳变，导致系统下电”故障模式，使用硬件故障注入方法设计测试用例开展测试，示例见表3。

表3 关键信号防抖处理测试用例

测试用例标识	GZZR-004	故障注入方法	硬件故障注入
测试用例名称	关键信号防抖处理	测试方法	边界值分析
测试追踪	FMECA-04		
测试说明	对软件中使用的硬件关键信号进行防抖处理，防止信号跳变导致的状态切换。		
测试过程			
序号	输入步骤	预期结果	实际结果
1	通过电源、信号源模拟下电中断信号高电平小于1 s。	系统异常下电。	系统异常下电。
2	在程序中增加对下电中断信号的防抖处理（该信号持续为高电平1 s以上时，才认为该信号有效）。通过电源、信号源模拟下电中断信号出现抖动。通过电源、信号源模拟下电中断信号高电平小于1 s。	系统未出现下电情况。	系统未出现下电情况。
通过准则	实际结果与预期结果一致	执行结果	通过

2.3 软硬件结合故障注入

软硬件结合故障注入是将硬件故障注入方法与软件故障注入方法相结合，在硬件故障注入设备的支持下通过其中加载的软件对电磁或电源干扰的信号源进行改变，从而达到比单纯使用硬件故障注入方法更加复杂的干扰方式[15]。

（1）构建软硬件结合故障注入环境

搭建软硬件故障注入平台，平台中包括软硬件故障注入设备及配套软件等。

（2）基于软硬件结合故障注入的测试设计

依据系统故障模式中的故障原因分析，设计测试用例中的软硬件激励条件，验证系统能够对典型故障模式正确处理。软硬件结合故障注入测试用例要素与软件故障注入测试用例要素一致。

（3）基于软硬件结合故障注入的测试方法

基于软硬件结合故障注入的测试方法的基本原理为：通过将软件故障注入手段与硬件故障输入手段相结合的方式，实现复杂的故障注入。如通过软件控制信号源产生特定噪声，同时对软件硬件进行故障注入，实现多种故障的同时注入，

（4）测试用例及执行结果样例

针对“软件从外部存储中读取内容错误的数据，导致系统无法识别”故障模式，使用软硬件结合故障注入方法设计测试用例开展测试，示例见表 4。

表 4 数据读取写入校验处理测试用例

测试用例标识	GZZR-005	故障注入方法	软硬件结合故障注入
测试用例名称	数据读取写入校验处理	测试方法	功能分解
测试追踪	FMECA-05		
测试说明	软件从 FLASH、EEPROM、NVM 等存储器中写入或读取数据时，增加校验位以确保写入及读取数据的正确性。		

测试过程			
序号	输入步骤	预期结果	实际结果
1	通过信号源、示波器向存储芯片施加异常电平。通过软件对存储芯片进行读写操作并查看读写结果。	软件对存储器芯片读写结果错误。	软件对存储器芯片读写结果错误。
2	在程序中增加对读写存储器的数据校验处理（按位进行奇偶校验，校验错误时进行提示）。通过信号源、示波器向存储芯片施加异常电平。通过软件对存储芯片进行读写操作并查看读写结果。	软件弹出提示信息，存储器读写操作异常。	软件弹出提示信息，存储器读写操作异常。
通过准则	实际结果与预期结果一致	执行结果	通过

2.4 总线故障注入

总线故障注入，即对系统外部交联设备故障注入技术，通过直接注入、仿真模型注入等方法，实现对系统外部输入 / 输出行为故障的模拟，验证系统对外部输入 / 输出的各类异常、故障及危险情况的检测、处理与隔离能力。

（1）构建总线故障注入环境

搭建总线故障注入平台，平台中包括总线故障注入设备及配套软件（如 CANoe）等 [16]。基本原理为通过总线故障注入设备软件配置总线故障注入设备输出异常数据，实现故障注入。总线故障注入设备包含的接口类型可以为 RS-232/422/485、CAN、ARINC429 等通用总线形式 [17-18]。

（2）基于总线故障注入的测试设计

依据系统故障模式中的故障原因分析，设计测试用例中的总线激励条件，验证系统能够对典型故障模式正确处理。总线故障注入测试用例要素与软件故障注入测试用例要素一致。

（3）基于总线故障注入的测试方法

总线故障注入方法包括总线接口黑盒测试技术，即通过复杂系统的外部总线和接口，向系统施加激励，并观察响应；面向动态数据内容的总线激励技术，测试内容包括总线协议和物理连接，注入数据传输层及其底层的故障，如总线中断、速率不匹配等；实时仿真故障注入技术，即建立数字仿真平台，通过数字仿真取代系统的真实外部交联环境连接 [19]。

（4）测试用例及执行结果样例

针对“总线数据流量超过总线性能指标要求，导致数据阻塞”故障模式，使用总线故障注入方法设计测试用例开展测试，示例见表 5。

表 5 总线负载处理测试用例

测试用例标识	GZZR-002	故障注入方法	总线故障注入
测试用例名称	总线负载处理	测试方法	边界测试
测试追踪	FMECA-02		
测试说明	根据数据重要程度设置适当的接口优先级及数据发送频率，减少总线负载。		

测试过程			
序号	输入步骤	预期结果	实际结果
1	通过总线故障注入工具，增加总线传输负载。通过软件向总线发送数据。	软件发送数据产生阻塞，系统通信中断。	软件发送数据产生阻塞，系统通信中断。
2	通过总线故障注入工具，逐渐降低总线传输负载。直至软件向总线发送数据不会产生阻塞。	得到总线传输负载允许的最大值。	得到总线传输负载允许的最大值。
3	减少总线连接设备的数据发送负载至允许的最大值后，通过软件向总线发送数据。	软件可以正常发送数据，不会产生阻塞，系统通信不会中断。	软件可以正常发送数据，不会产生阻塞，系统通信不会中断。
通过准则	实际结果与预期结果一致	执行结果	通过

3 工程应用验证

针对典型雷达系统故障模式，选择适用的验证方法进行安全性测试，优先使用可信度最高的安全性测试方法。同时，也需要考虑故障注入方法中验证环境配置及实际测试执行的难度。本文结合某典型雷达的软件安全性测试开展工程应用研究。

选取两个雷达软件系统测试项目和两个配置项测试项目，将测试人员随机分为两组，分别使用传统的测试方法和基于故障注入的安全性测试方法开展软件安全性测试工作。统计两组发现的软件安全性缺陷个数。项目验证统计数据如表 6 所示。

表 6 测试设计和测试结果数据统计

项目名称	传统测试方法 测试发现缺陷	故障注入方法 测试发现缺陷
系统测试项目 1	5	7
系统测试项目 2	9	13
配置项测试项目 1	10	15
配置项测试项目 2	5	9

由上述工程应用示例可知，本文提出的基于故障注入的雷达软件安全性测试方法可实现对典型雷达系统故障模式的有效验证，提高软件安全性缺陷的检出率，有效保障雷达系统的安全性。

4 结论

本文提出一种基于故障模式的雷达软件安全性测试方法。首先，针对收集典型历史雷达系统故障数据进行总结与分析，形成典型雷达系统故障模式，并从输入故障、输出故障、程序处理故障等角度对故障模式进行分类。在故障模式基础上，形成基于故障注入的雷达系统安全性测试方法，可以实现对故障模式的有效验证。最后，针对某典型雷达系统故障数据，进行工程应用研究。研究成果表明，本文所提出的基于故障注入的软件安全性测试方法可以有效提升雷达系统对典型系统故障和问题的保护能力，降低系统运行故障率，具有较好的工程操作性和可行性，提升雷达软件的安全性。

参考文献：

[1] 莊露 , 陆中 , 宋海靖 , 等 . 基于故障注入模型的电传飞控系统安全性分析 [J]. 航空学报 , 2023,44(9):327329.

[2] 李昊 , 田峰敏 . 雷达软件的安全性测试研究 [J]. 信息化研究 , 2011, 37(6):29-33.

[3] 叶婷 , 曾幸钦 , 刘惠玲 , 等 . 面向需求的软件安全性测试方法 [J]. 电子元器件与信息技术 , 2021,5(10):168-169.

[4] 张风玲 , 胡逸琳 , 代晓倩 , 等 . 嵌入式软件安全性测试研究 [J]. 软件 ,2024,45(01):184-186.

[5] 赵昶宇 . 嵌入式软件安全性测试技术研究 [J]. 科技与创新 , 2023(21): 87-89.

[6] 李震 , 张勇 . 基于最小割集的软件安全性测试用例生成 [J]. 计算机与数字工程 , 2019, 47(7): 1772-1775.

[7] 董燕 , 王小丽 . 一种星载嵌入式软件安全性测试方法 [J]. 测控技术 , 2016,35(4):117-119.

[8] 幺飞 , 时光 , 富小薇 . 基于故障注入技术的航天器系统级软件测试方法研究 [J]. 航天器工程 ,2019,28(1):130-136.

[9] 姜文 , 刘立康 . 基于故障注入的应用软件可靠性测试 [J]. 计算机技术与发展 , 2019,29(2):23-28.

[10] 乔邦江 , 刘彪 , 易泽鹏 , 等 . 基于软件故障注入的系统验证测试评估技术研究 [J]. 航空维修与工程 ,2023,(12):36-40.

[11] 董志腾 . 面向复杂环境的软错误故障注入和检测技术研究 [D]. 南京 : 南京航空航天大学 ,2021.

[12] 曲晨冰 , 王乃晔 , 王力纬 , 等 . 通信芯片电压故障注入测试与功能安全评估方法 [J]. 智能安全 ,2023,2(3):85-92.

[13] 刘强 , 李一可 . 基于指令扩展的 RISC-V 可配置故障注入检测方法 [J/OL]. 北京航空航天大学学报 ,1-13[2024-09-13]. https://doi.org/10.13700/j.bh.1001-5965.2022.0995.

[14] BAILAN, OSCAR, ROSSI, UMBERTO, WANTENS, ANNE, et al. Verification of soft error detection mechanism through fault injection on hardware emulation platform[C]. //International Conference on Dependable Systems and Networks Workshops (DSN-W 2010).:IEEE, 2010:113-118.

[15] 张春侠 , 周春梅 , 董文杰 . 软硬件结合的嵌入式故障注入试验系统研究 [J]. 核电子学与探测技术 ,2013,33(5):586-589.

[16] 廖建造 , 王磊 , 毛艺 基于 CAPL 的 CAN 总线故障注入自动化测试系统设计 [J]. 上海汽车 , 2023 (4) : 21-26.

[17] 闫淑群 , 张鹏 , 罗宇辉 , 等 . 基于 FPGA 的弹箭多种通讯总线故障注入和自动诊断系统的设计与实现 [J]. 计算机测量与控制 , 2024,32(6):65-70.

[18] 刘鹤 , 张晓明 , 张月 . 基于总线故障注入的卫星热控自主管理软件测试方案 [J]. 航天器工程 ,2024,33(3):135-140.

[19]SUN L, XU P.Design and implement of RS-485 bus fault injection[C]//International Conference on Reliability, Maintainability and Safety (ICRMS 2011). Piscataway: IEEE, 2011: 975-980.

【作者简介】

赵国利（1991—），男，山东聊城人，硕士，工程师，研究方向：软件工程。

（收稿日期：2024-07-06）