ICS 35.080
CCS L 77

T/CICC

中 国 指 挥 与 控 制 学 会 团 体 标 准

T/ CICC 35017—2025

复杂软件系统抗辐射技术要求

Technical requirements for anti-radiation complex software systems

2025-11-20 发布　　2025-11-20 实施

中国指挥与控制学会　发布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语与定义 1
4 缩略语 3
5 软件抗辐射要求 3
5.1 一般要求 3
5.2 定性要求 3
5.3 定量要求 4
6 软件抗辐射技术要求适用对象 4
6.1 数据 4
6.2 可执行文件 4
6.3 配置文件 4
6.4 日志文件 4
6.5 寄存器 4
6.6 内存与存储器 4
6.7 通信接口 4
7 复杂软件系统抗辐射风险分析及监测 4
7.1 抗辐射风险分析 4
7.1.1 关键功能风险分析及排序 4
7.1.2 关键模块风险分析及排序 5
7.1.3 关键数据风险分析及排序 6
7.1.4 综合分析 7
7.2 抗辐射风险监测机制 7
7.2.1 监测点布置及数据采集 7
7.2.2 监测规则 8
7.2.3 监测数据分析 8
8 复杂软件系统抗辐射加固设计 9
8.1 刷新加固 9
8.2 冗余加固 9
8.3 定期自检 10
8.4 错误检测与纠错 10
8.5 分区机制 10
9 复杂软件系统抗辐射仿真测试 10
9.1 概述 10
9.2 测试对象 10
9.3 测试模型 10
9.3.1 故障注入策略 10

9.3.2 故障注入工具 11
9.3.3 仿真测试结果分析 11
10 复杂软件系统物理辐照试验 11
11 复杂软件系统抗辐射评估 12
11.1 小样本评估 12
11.2 等效评估 13
11.3 迁移评估 13
参 考 文 献 15

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国指挥与控制学会提出并归口。

本文件起草参与单位：北京航空航天大学、杭州市北京航空航天大学国际创新研究院（北京航空航天大学国际创新学院）、中国星网网络创新研究院有限公司、可靠性与环境工程技术国家级重点实验室、北京航空航天大学可靠性工程研究所、北京智慧云测设备技术有限公司。

本文件主要起草人：杨顺昆、邵麒、张杰一，徐磊，门良知、李晓亮、杜磊、周怡婧、吴梦丹。

复杂软件系统抗辐射技术要求

1 范围

本文件规定复杂软件系统抗辐射的定性与定量要求、支撑技术与方法，包括风险分析和监测、软件加固设计、仿真测试和评估。

本文件适用于复杂软件系统全生命周期的抗辐射活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34956－2017 大气辐射影响 航空电子设备单粒子效应防护设计指南

GB/T 34955－2017 大气辐射影响 航空电子系统单粒子效应试验指南

GB/T 40134-2021 航天系统电磁兼容性要求

GB/Z 37150-2018 电磁兼容可靠性风险评估导则

GB/T 41270.7－2022 航空电子过程管理 大气辐射影响 第 7 部分：航空电子产品设计中单粒子效应分析过程管理

QJ 10005－2008 宇航用半导体器件重离子单粒子效应试验指南

3 术语与定义

GB/T 25000.21－2019、GB/T 11457－2006 和 GJB/Z 161－2012 确立的以及下列术语和定义适用于本文件。

3.1

复杂软件系统 complex software system

由大量相互依赖、相互作用的软件组件（计算机程序、模块、服务等）通过复杂的逻辑和物理关系连接而成，并遵循严格的规程（流程、协议、策略）进行协同运作，需动态应对内外部软件、硬件与环境的变化以实现复杂业务或关键领域目标的软件集成。其本质特征在于结构庞大、功能多样、环境多变、动态交互、任务复杂，通常具备多层次架构、模块协作、高度耦合以及较长的生命周期。

3.2

单粒子效应 single event effect

单个粒子（如太阳高能粒子、高能中子和质子）入射器件产生的响应。

注：响应包括：非破坏性（如翻转）和破坏性的（如锁定和栅穿）现象。

[来源：GB/T 34956－2017，3.53]

3.3

软失效 soft failure

允许具有部分操作能力的系统继续操作的失效。

[来源：GB/T 11457－2006，2.1468]

3.4

软错误　soft errors

锁存器或存储单元中的错误输出信号可以通过该器件针对该锁存器或存储单元执行一个或多个正常功能后加以纠正的现象。

注 1：通常，这一术语一般指辐射或电磁脉冲诱发的错误，并非指制造加工过程中引入物理缺陷导致的错误。

注 2：SEU，SEFI，MBU，MCU 和 SET 会产生软错误。商用行业采用软错误（SER）这一术语，而航空电子系统、航天与军用系统领域一般采用更专业的术语如 SEU、SEFI 等。

注 3：术语“软错误”首次由 Intel 公司的 May 与 Woods（针对 DRAM 与集成电路 IC）在其 1978 年 4 月国际可靠性物理年会 IRPS 上提出，而术语“单粒子翻转”由 NRL 的 Guenzer, Wolicki 与 Allas 在其 1979 年 NSREC 论文《中子与质子诱发 DRAM 单粒子翻转》中引入。

[来源：GB/T 34956－2017，3.60]

3.5

单位翻转　single bit upset

半导体器件吸收足够辐射导致单个单元逻辑状态发生改变的现象。

[来源：GB/T 34956－2017，3.50]

3.6

多位翻转　multiple bit upset

单个电离粒子在电子器件中硅材料上沉积能量，导致同一个字中不止一个比特位发生翻转的现象。

[来源：GB/T 34956－2017，3.39]

3.7

多单元翻转　multiple cell upset

单个电离粒子在电子器件中硅材料上沉积能量, 诱发集成电路(IC) 中几个比特位同时发生翻转的现象。

[来源：GB/T 34956－2017，3.40]

3.8

单粒子锁定　single event latch-up

含有最少 4 层半导体 p-n-p-n 结构的器件，吸收足够辐射后，导致无论怎样施加输入，在某节点上始终维持一个固定的状态直至器件断电的现象，可能是破坏性现象，也可能是非破坏性现象。

3.9

单粒子功能中止　single event functional interrupt

通常指在复杂器件（如微处理器）中发生翻转，引起控制路径被改变，导致器件停止运行正常功能的现象。

3.10

软件崩溃　software crash

计算机系统或部件的突然的和完全地失效。

[来源：GB/T 11457－2006，2.362]

3.11

软件挂起　software hang

软件在运行过程中因某些原因导致程序停止响应用户的操作，但并未完全终止运行的现象。挂起的程序通常表现为界面无响应、无法进行正常交互，但进程仍在后台运行且可能占用系统资源。

3.12

静默数据损坏　silent data corruption

在没有触发任何错误报告或警告的情况下，存储系统中数据发生错误性改变的现象。

3.13

风险　risk

在规定的成本、时间及技术参数内达到整个计划目标的潜在失效的度量。

[来源：GB/T 34956—2017，3.49]

3.14

故障注入　fault injection

故障注入是一种软件测试技术，通过有意地在系统中引入故障（如错误输入、硬件失效、异常条件等），评估软件或系统在异常情况下的行为表现，以验证其鲁棒性、容错能力和可靠性。

4　缩略语

下列缩略语适用于本文件：

EDAC　错误检测与纠错（Error Detection and Correction）
FMEA　故障模式和影响分析（Failure Mode and Effects Analysis）
SDC　静默数据损坏率（Silent Data Corruption Rate）
SEE　单粒子效应（Single Event Effect）
SEU　单粒子翻转（Single Event Upset）
SFTA　软件故障树分析（Software Fault Tree Analysis）
SFMEA　软件故障模式和影响分析（Software Failure Mode and Effects Analysis）
MBU　多位翻转（Multiple Bit Upset）
MCU　多单元翻转（Multiple Cell Upset）

5　软件抗辐射要求

5.1　一般要求

在寿命周期内，复杂软件系统及其所有子系统应具备良好的抗辐射能力，能够在不同辐射环境（如大气辐射、深空辐射或者电磁辐射环境下）中持续、稳定地运行，不发生功能紊乱、性能退化或系统故障。系统应在软件层面有效应对粒子翻转或者锁死等常见辐射诱发故障，并具备相应的检测、恢复与容错机制。对于涉及系统安全的关键功能和任务控制逻辑，应在实际使用前验证其在目标辐射环境下的辐射容忍性，确保具备足够的抗辐射安全裕度，并满足系统级抗辐射兼容性要求。

本标准主要针对辐射环境下复杂软件系统可能发生的故障或失效，提出相应的软件抗辐射定性和定量要求、适用对象、辐射风险分析及监测方法、复杂软件系统抗辐射加固设计、复杂软件系统抗辐射仿真测试、物理辐照试验流程及分析评估。为复杂软件系统在不同辐射环境下的鲁棒性评估与抗辐射能力设计提供依据。

5.2　定性要求

定性评估侧重于软件的稳定性、健壮性及关键功能的容错能力，确保在不同辐射环境下，软件不发生非预期故障，不影响任务执行或数据完整性。具体要求如下：

a）　应通过辐射试验或仿真测试实验证明软件在辐射环境下不出现崩溃或者挂起的现象；
b）　应保证软件关键功能、关键模块、关键数据具有抵抗被干扰的保护能力；
c）　应保证软件静默数据损坏出现时不应影响软件的关键功能；
d）　在辐射环境下，软件在信息交互过程中若出现通信异常，如命令格式错误、数据接收超时；
e）　软件应具有返回错误状态信息的功能，保证其软件的正常运行；
f）　面向辐射效应的故障监测方式不引起被加固软件系统的关键性能受损。

5.3 定量要求

软件抗辐射定量评估主要关注软件在辐射环境下的稳定性、完整性和功能可用性。具体要求如下：

a） 静默数据损坏率：表示在辐射环境下，程序正常运行但因软错误输出错误数据的频率；
b） 挂起率：表示由于软错误导致程序进入死循环或长时间无响应的频率；
c） 崩溃率：表示由于软错误引起程序崩溃发生的频率；
d） 故障容忍度：用于衡量软件能够容忍软错误的能力；
e） 失效率：表示由于软错误导致软件系统功能失效的频率；
f） 需要评估空间冗余类加固方案对被加固程序性能影响。

6 软件抗辐射技术要求适用对象

6.1 数据

应对软件系统易受辐射干扰影响的输入数据、输出数据、内部状态数据、配置数据等关键数据进行辐射干扰风险分析、加固设计与测试验证。

6.2 可执行文件

应对软件系统的可执行文件进行辐射干扰风险分析、加固设计与测试验证，确保其在安装、使用和存储过程中不受辐射干扰破坏。

6.3 配置文件

应对软件系统中可能存在的配置文件进行辐射干扰风险分析、加固设计与测试验证，确保其在安装、使用和存储过程中不受辐射干扰破坏。

6.4 日志文件

应对软件系统中可能存在的日志文件进行辐射干扰风险分析、加固设计与测试验证，确保其在使用和存储过程中不受辐射干扰破坏。

6.5 寄存器

应对软件系统中使用的关键寄存器进行辐射干扰风险分析、加固设计与测试验证，确保其在使用过程中不受辐射干扰破坏或降低辐射干扰破坏的影响。

6.6 内存与存储器

应对软件系统中使用的内存和存储单元进行辐射干扰风险分析、加固设计与测试验证，确保其在使用过程中不受辐射干扰破坏或降低辐射干扰破坏的影响。

6.7 通信接口

应对软件系统中使用的通信接口（串口、网络、总线、数字量、模拟量等）进行辐射干扰风险分析、加固设计与测试验证，确保其在使用过程中不受辐射干扰破坏或降低辐射干扰破坏的影响。

7 复杂软件系统抗辐射风险分析及监测

因复杂软件系统具有高耦合、高复杂和高动态等固有特性，系统在运行过程中面临多源输入扰动、状态转移路径庞杂及模块间连锁反应等多维挑战，极易在辐射环境中诱发异常行为。为有效识别和控制辐射引发的潜在风险，应优先从“关键功能、关键数据和关键模块”三个维度出发，开展系统级的风险识别与分级评估。

7.1 抗辐射风险分析

首先应从关键功能、关键数据和关键模块三个方面识别辐射风险敏感性并进行排序，给出防护或测试的重点对象。

7.1.1 关键功能风险分析及排序

7.1.1.1 关键功能识别

关键功能的识别应从以下两个方面进行系统分析：

a） 任务关键型功能识别，识别在系统运行过程中承担核心业务逻辑、任务控制或安全保障职责的功能模块，具体判断标准包括：

1） 安全性：功能是否直接关系系统的安全控制、数据完整性或访问权限管理，且其失效是否可能导致信息泄露、数据损坏或安全防护失效等严重后果；

2） 业务关键性：功能是否处于主要业务流程或核心任务链中，对任务执行的连续性、完整性具有关键支撑作用；

3） 运行稳定性：功能在异常条件下是否可能引发系统死循环、资源阻塞、程序崩溃或关键流程中断，影响系统的稳定运行；

4） 核心依赖性：功能是否作为系统运行的基础模块，其正常工作是否为其他模块、子系统或任务逻辑所必需。

b） 辐射敏感性功能识别，识别在辐射环境中易受单粒子翻转、多位翻转等软错误影响，且与其他模块存在复杂依赖关系的功能模块。识别依据包括：

1） 是否依赖易受辐射影响的资源（如关键寄存器、中断向量、状态位等）；

2） 是否存在复杂状态转换逻辑，易因位翻转导致控制流异常；

3） 是否与多个模块存在强数据耦合或控制依赖，潜在影响范围广。

7.1.1.2 关键功能风险排序

关键功能风险排序具体要求如下：

a） 对功能的失效风险进行量化评估（如可能的故障频率与系统影响）；

b） 对易受辐射影响的高敏感性功能进行排序；

c） 根据以上两种分析结果，给出关键功能风险和辐射敏感性排序结果。

7.1.2 关键模块风险分析及排序

7.1.2.1 关键模块识别

关键模块识别具体要求如下：

a） 软件系统中，实现核心功能、保障系统稳定性和安全性至关重要的模块；

b） 根据对系统整体功能和安全性的重要性，定义“关键模块”的标准，还可参考下述评判依据：

1） 模块是否涉及核心逻辑（如控制算法、数据处理等）；

2） 模块是否与外部交互紧密（如传感器数据读取、输出控制）；

3） 软件故障树分析（SFTA）；

4） 软件失效模式和影响分析（SFMEA）。

c） 辐射敏感型模块识别，其判断依据包括：

1） 模块是否依赖易受辐射影响的关键结构资源，如中断向量、状态变量、软寄存器、堆栈指针等；

2） 模块内部是否包含复杂的状态控制逻辑、条件跳转结构、深度嵌套流程等，导致辐射失效难以恢复；

3） 模块是否缺乏冗余设计、自恢复机制或错误检测手段（如无TMR、无ECC、无软错误监测机制）；

4） 模块是否处于失效传播链的起点或中继节点，具备系统级影响范围。

7.1.2.2 关联分析

关键模块的关联分析具体方法如下：

a） 根据 7.1.1.2 中分析得出的关键功能列表映射到模块，确定模块间的数据传递关系，识别哪些

模块是核心数据的来源；

b） 使用工具生成模块调用图，标注模块之间的依赖关系，找出依赖度高或被多个模块调用的模块，这些模块通常是关键模块；

c） 分析模块可能出现的故障类型及其概率。

7.1.2.3 风险分析及排序

风险分析及排序的具体方法如下：

a） 基于复杂性指标分析模块风险：根据模块复杂性指标（如代码行数、圈复杂度、模块耦合性等）评估模块的复杂性并确定潜在风险；

b） 利用维护历史识别关键模块：通过版本控制工具查看模块的变更频率和历史缺陷记录，变更频繁或缺陷多的模块可能是关键模块；

c） 量化风险值：对每个关键模块进行粒度分析，量化每个关键模块的翻转风险（如错误率、系统影响程度），并生成风险值；

d） 模块排序与优先级：根据量化的风险值和辐射敏感性对关键模块进行排序，明确哪些模块需要优先优化。

7.1.3 关键数据风险分析及排序

7.1.3.1 关键数据识别

关键数据识别的类型具体要求如下：

a） 任务关键型数据识别：

1） 功能依赖性：系统核心功能是否直接依赖该数据进行控制决策、流程转移或执行判断；

2） 业务流程关键性：数据是否贯穿飞控主流程、导航计算、资源调度等核心任务；

3） 系统稳定性影响：数据错误或丢失是否可能导致任务中断、控制跳变、死循环等严重后果；

4） 多模块耦合性：数据是否为多个模块共享或交互使用的关键数据中枢，其异常是否可引发模块间级联故障。

b） 辐射敏感型数据识别：

1） 物理易失性：数据是否存储在易受单粒子翻转（SEU）、多位翻转（MBU）影响的资源中（如SRAM变量、未加ECC保护缓冲区、堆栈等）；

2） 控制路径关联性：数据是否用于控制分支判断、状态转换、条件跳转等控制流敏感位置，若翻转将导致严重逻辑偏转；

3） 无容错机制保障：数据是否缺乏奇偶校验、CRC校验、定期刷新、三模冗余（TMR）等保护机制，失效后不可被系统主动发现。

7.1.3.2 梳理系统数据流

数据流分析的具体方法如下：

a） 分析数据的来源和用途：

1） 列出系统所有的数据来源（如数据库、用户输入、外部接口）；

2） 确定每种数据的流向，包括传递到哪些模块、被哪些功能使用。

b） 绘制数据流图：

1） 使用工具绘制系统的数据流图，展示数据在模块之间的传递路径。（针对不同语言利用开源工具生成对应的数据流图）；

2） 标注数据流中的关键节点（如输入处理、存储、输出等）。

7.1.3.3 分类整理数据

整理数据的类别具体要求如下：

a） 输入数据：用户输入的数据（如表单信息、命令），外部系统传入的数据（如 API 响应）；

b） 处理数据：系统内部生成或加工的数据（如中间结果、临时变量）；

c） 存储数据：数据库中持久化存储的数据（如用户信息、交易记录）；

d） 输出数据：系统对外输出的数据（如报表、结果显示），标记每类数据的重要性，并重点分析存储数据和核心逻辑相关的处理数据。

7.1.3.4 识别软件关键数据

软件关键数据识别的要求如下：

a） 模块间依赖：分析模块之间的数据依赖关系，确定哪些数据被多个模块共享或依赖。被多个模块频繁调用或依赖的数据通常是关键数据；

b） 数据间关联：找出数据之间的关联关系（如主从表、外键），如果某数据被用作其他数据的计算基础或验证条件，则该数据可能为关键数据；

c） 基于复杂网络的关键数据识别。

7.1.3.5 关键数据风险排序

关键数据风险排序的过程如下：

a） 根据数据粒子翻转可能性和影响范围，评估数据的风险级别；

b） 对关键数据风险和辐射敏感性按优先级排序。

7.1.4 综合分析

抗辐射风险的综合分析过程如下：

a） 汇总关键功能、关键模块和关键数据的风险和辐射敏感性排序结果；

b） 结合实际工程需求和资源限制，提出以下措施：

1） 设计改进：优化硬件设计或软件逻辑，降低粒子翻转影响；

2） 冗余设计：增加关键部件或数据的备份和容错能力；

3） 屏蔽防护：对易受粒子翻转影响的部件添加屏蔽保护措施；

4） 监测与修复：引入实时监测机制，快速发现和纠正粒子翻转错误；

5） 给出重点防护、仿真测试和实验验证的功能、模块和数据部分。

7.2 抗辐射风险监测机制

7.2.1 监测点布置及数据采集

7.2.1.1 确定监测目标

监测目标的定义和优先级要求如下：

a） 目标定义：

1） 明确监测的粒子翻转现象（如单比特翻转、单粒子锁定、单粒子功能中止等）；

2） 结合系统特点，确定需要监测的核心数据或状态（如存储数据完整性、寄存器状态、功能运行正确性）。

b） 目标优先级：

1） 优先监测关键模块和关键数据所在区域（如内存、缓存、寄存器）；

2） 对重要的系统功能（如安全机制、数据校验机制）加大监测力度。

7.2.1.2 监测点布局

监测点布局的原则、布置和数据采集机制要求如下：

a） 布置原则：

1） 高风险区域优先：选择发生粒子翻转的高风险区域（如高辐射区域、敏感硬件模块）；

2） 覆盖核心模块：确保系统中关键模块和数据操作区域有足够的监测点；

3） 考虑冗余性：避免因监测点失效导致监测盲区。

b） 监测点布置：

1） 硬件层监测点布置：在内存、寄存器、处理器缓存等关键硬件单元布置监测电路（如探测器\专用硬件模块）；使用可编程逻辑器件（如FPGA）实现粒子翻转实时检测电路。

2） 软件层监测点布置：在关键数据操作代码中加入检查点（如关键变量读写时插入校验逻辑）；在核心算法流程（如状态机）添加断言或日志记录点。

3） 选择监测点的工具支持：使用系统仿真工具（如辐射环境模拟）预测粒子翻转高发区域，辅助监测点布置；分析系统中最容易发生比特翻转的区域，如高辐射环境或关键硬件模块（如内存、寄存器）。

c） 数据采集机制：

1） 选择采集工具：硬件工具：利用探测器（如辐射监测仪或专用检测芯片）记录单粒子事件；软件工具：使用实时数据采集框架记录关键变量的值。

2） 设定采样频率：根据系统运行特性确定数据采集频率，确保不遗漏关键翻转事件；确定存储和传输方案（如将数据传输至中央数据库或本地存储）；高实时性场景（如航空航天系统）需要高频采样，非实时场景可适当降低频率。

3） 数据存储与标记：数据存储应包括时间戳、监测点位置、翻转事件特征值等；

4） 异常标记与报警：在采集到粒子翻转事件后，立即标记异常数据并触发报警；支持实时监控界面展示异常信息。

7.2.2 监测规则

监测规则设定的具体要求如下：

a） 确定正常阈值范围：

1） 根据系统设计规格，确定关键变量的正常值或运行状态范围；

2） 结合历史数据，识别翻转可能导致的异常特征（如数值突变、指针错误等）。

b） 制定异常检测标准：

定义比特翻转的判定标准，例如：

1） 数据位发生单点翻转（如二进制位从0变为1）；

2） 变量值超出预期范围（如重要参数值突然增大或变为负数）；

3） 使用容错校验码（如奇偶校验、哈希校验）设计监测机制；

4） 指针或地址异常（如指向无效内存区域）。

c） 动态监测与规则优化

1） 结合实时运行数据，动态调整监测规则；

2） 定期更新规则库，纳入新的故障模式或异常类型。

7.2.3 监测数据分析

监测数据的分析方法如下：

a） 数据分析方法：

1） 应用统计学方法（如异常值检测）分析监测数据，识别潜在比特翻转事件；

2） 利用机器学习算法（如分类器）建立粒子翻转特征模型。

b） 多源数据融合

综合不同监测点的多源数据（如硬件探测器数据与软件日志），提高判定准确性。

c） 误报与漏报分析：

1） 针对误报和漏报情况，优化算法和规则，降低误报率，提高异常检测覆盖率；

2） 在采集的数据中标注异常事件，便于后续分析。

8 复杂软件系统抗辐射加固设计

8.1 刷新加固

复杂软件系统应具备刷新机制，具体要求如下：

a） 定时刷新：

1） 应按照预设周期自动执行数据刷新操作；

2） 刷新周期应支持手动配置，并可根据数据重要性采用分级策略；对核心数据应设置更高频度的刷新周期，对普通数据可设置较低频度的刷新周期，从而实现多级周期管理策略。

b） 遥控刷新：

1） 应采用密码与动态令牌相结合的双因素身份验证机制，确保指令发起方的合法性；

2） 应对远程刷新操作实施权限分级管理，防止未经授权的访问；

3） 刷新指令的传输过程应采用加密通信协议，防止信息在传输过程中被篡改或泄露。

c） 动态触发刷新：

1） 应支持基于事件触发的数据自动刷新机制；

2） 系统应能够在特定事件发生时（如系统启动、数据修改或异常告警）自动执行数据刷新操作，并应支持对可触发自动刷新的事件类型进行配置与管理。

d） 回读校验：

1） 应在数据读取后执行完整性校验；若校验失败，应自动进行数据重写操作；

2） 系统应支持配置多种校验算法（如校验和、哈希校验等），并允许按需选择。若连续校验失败次数超过3次，应触发异常告警机制，并记录相关事件信息以供后续分析；

3） 对于每一次的刷新，需要记录刷新的日志；包括刷新类型、刷新角色、刷新对象、响应结果等；对于刷新失败的情形，应确保数据可以回滚至上一有效状态；对于连续三次的刷新失败情况，应该触发异常处理模块。

8.2 冗余加固

冗余存储加固建议采用如下方式：

a） 对存储空间较小的变量，遵循以下流程：

1） 每个变量应存储三份副本，且应分布于内存中不连续的存储块，以降低多位翻转影响；

2） 读取时，采用“三取二”表决法对三份副本进行一致性比对；若三者中有两者一致，则将该值作为有效值，并用其覆盖不一致的副本；

3） 写入时，应同时更新三份副本，并在写入后进行回读校验，以确保值更新成功并一致。

b） 对存储空间较大的变量，遵循以下流程：

1） 对存储空间较大的变量（如结构体、数组、缓冲区等），应采用“副本+哈希校验”的方式增强容错能力；

2） 应存储2至3份副本（设为N份），每份副本应包括变量本体与其哈希值；

3） 各副本应尽量存储在内存的随机或物理隔离位置；

4） 写入时，应在每个副本写入后立即生成哈希值，并与变量一同存储；所有副本写入完成后，应校验其哈希值是否一致；若一致则写入成功，若存在不一致，应重新执行写入流程；

5） 读取时，应逐个验证副本的哈希值是否与当前变量值匹配，若找到一致副本则以其为准，并用于覆盖其他副本；若所有副本哈希均校验失败，则视为数据已严重损坏，系统应触发应急错误处理流程。

8.3 定期自检

在辐射环境下，复杂软件系统应对关键器件及其数据状态进行周期性完整性校验。具体要求如下：

a） 定期自检机制应覆盖以下关键部件与模块：寄存器、存储器、传感器、FPGA、内存单元以及其他专用硬件模块等。

b） 应根据存储器所在模块的功能重要性与辐射敏感性，实施分级管理，并配置相应的自检频率与容错阈值。

8.4 错误检测与纠错

复杂软件系统抗辐射应具备有效的错误检测与纠错机制（EDAC），识别和修正数据在传输或存储过程中因辐射效应引发的单比特或多比特错误。具体方法如下：

a） 应根据具体系统的关键性、安全性及资源限制，合理选取适配的 EDAC 算法，并在硬件或软件层实现对应的检测与恢复流程。

b） 单比特错误检测与纠正：应采用如基本海明码、扩展海明码、缩短海明码、增强型海明码等方法，具备低资源占用、快速识别与修复的能力；

c） 多比特错误检测与纠正：可采用里德-所罗门码（RS 码）、BCH 码、循环冗余校验码（CRC）、TURBO 码等机制，并结合内存巡检策略进行周期性检测与动态纠错。

8.5 分区机制

对关键的功能、模块和数据，建议在系统设计时考虑时间分区、空间分区、资源分区和混合分区等方法进行管理与隔离。

9 复杂软件系统抗辐射仿真测试

9.1 概述

复杂软件系统抗辐射仿真测试主要是通过故障注入来实现，通过在程序执行过程中干扰或修改程序执行状态来模拟真实世界可能发生的软错误，并通过观察程序之后的运行情况，分析软错误对程序带来的影响，并以此对软件系统的抗辐射能力进行评估。

9.2 测试对象

复杂软件系统抗辐射仿真测试的对象主要是基于之前风险分析中识别的关键模块和关键数据，并覆盖寄存器级、指令级、IR 级（中间表示级）、源代码级和系统级等级别的对象范围。

9.3 测试模型

9.3.1 故障注入策略

在进行复杂软件系统抗辐射仿真测试时，故障注入策略需要考虑多个方面，以确保测试的有效性和针对性。具体考虑如下：

a） 比特翻转个数：应确定在测试过程中每次注入故障时翻转的比特数量；可以根据测试需求选择单比特翻转或多比特翻转，以模拟不同程度的软错误；

b） 比特翻转方向：指定比特翻转的方向，即从 0 翻转到 1 或从 1 翻转到 0，用于评估不同方向的翻转对系统行为的影响；

c） 故障注入位置：确定故障注入的具体位置，如寄存器、内存地址、数据总线等；

d） 故障注入时机：选择在程序执行的哪个阶段注入故障，如指令执行期间、数据传输过程中或特定任务的关键时刻，模拟真实环境中可能发生的故障时机；

e） 故障持续时间：设定故障的持续时间，可以是瞬时的或者持续的，这有助于评估软件系统对瞬时和持续故障的容忍能力；

f） 故障触发方式：考虑如定时触发、事件触发和随机触发等方式。

9.3.2 故障注入工具

在进行复杂软件系统抗辐射仿真测试中，故障注入工具的选择和使用对于测试的有效性和准确性至关重要，应覆盖寄存器级、指令级、IR 级（中间表示级）、源代码级和系统级五大类，并满足以下要求：

a） 应能够精确控制故障的类型、作用位置和影响范围，以确保测试的准确性；

b） 应允许用户自定义故障参数，并确保实验的可重复性；

c） 不应对正常执行流程产生额外干扰；

d） 应支持自动化执行，允许编写脚本控制故障注入过程，实现大规模测试和批量分析；

e） 应具备详细的日志记录功能，包括故障发生时间、位置、类型和结果等。

9.3.3 仿真测试结果分析

在复杂软件系统抗辐射仿真测试中，测试结果是评估软件系统在辐射环境下表现的关键步骤，主要考虑以下步骤：

a） 应收集故障注入过程中系统产生的所有异常数据和正确结果（作为对比基准），包括输出结果、错误日志、系统状态等；

b） 应将故障注入结果与正确结果进行对比，识别出差异和异常。注意以下异常结果：

1） 软件崩溃：程序在运行过程中因软错误而提前终止，无法完成预期任务；

2） 软件挂起：程序因软错误进入死循环或超时，无法继续执行或完成；

3） 静默数据损坏：程序能够正常执行至结束，但最终输出结果错误，且系统未报告任何异常。

c） 应对测试结果进行统计分析，综合计算 5.3 节中所提的定量指标，以进行全面分析。

10 复杂软件系统物理辐照试验

单粒子效应试验可参考 GB/T 34955－2017、电磁辐射试验可参考 IEC 61000、CISPR、MIL-STD-461 等，基本步骤和需要考虑的条件如下：

a） 试验准备，具体包括以下步骤：

1） 明确试验对象：器件或（和）电路板；

2） 确定试验类型：静态或动态（适用于大多数的板级试验）；

3） 选择适宜的辐射源，如中子、质子、电磁辐射源；

4） 组建试验团队；

5） 编制试验方案。

b） 试验实施，具体包括以下步骤：

1） 设备布置：根据试验方案布设试验对象与辐射源的空间关系，确保距离、角度、屏蔽等条件满足设计要求；

2） 接口连接：将试验对象与监控系统、供电系统、信号采集系统连接，确保电气接口安全可靠；

3） 功能初始化：对被试对象进行启动、配置与功能加载，确保试验前系统处于正常工作状态；

4） 辐照执行：按照设定剂量率、时间、粒子能谱等参数实施辐射，过程中持续监测器件状态、功能响应及输出结果；

5） 事件记录：完整记录试验过程中的功能失效事件、数据翻转现象、电流异常、复位触发等情况，形成原始试验数据集；

6） 多次重复：对重点器件或敏感路径应实施多次重复试验，以获取统计意义上的失效率指标。

c） 试验结果分析，应对采集数据进行分类处理和失效归因，具体包括：

1） 数据整理：汇总试验过程中记录的所有事件信息，包括功能异常时间点、异常持续时间、恢复方式等；

2） 事件分类：根据现象类型区分为软错误（如单粒子翻转SEU）、硬错误（如器件锁死、永久损伤）及可恢复性事件等；

3） 故障定位：结合波形、日志和功能输出，定位出故障对应的电路模块、功能单元或具体寄存器位；

4） 敏感性评估：根据事件出现频次、失效类型及功能影响，评估试验对象对不同辐射类型的敏感性；

5） 风险研判：根据故障类型、影响范围与系统容错能力，对目标功能或模块进行风险分级，为加固设计或冗余配置提供依据。

11 复杂软件系统抗辐射评估

开展复杂软件系统的抗辐射分析和评估工作时，受限于试验条件、资源成本以及参数空间维度等因素，通常难以依赖单一评估方法获取全面、准确且高效的评估结论。针对不同场景下的数据可获取性、评估粒度要求与分析目标，建议综合采用小样本评估、等效评估娇儿迁移评估三类具有互补特征的评估方法。

11.1 小样本评估

小样本评估的核心在于充分利用有限观测信息，结合统计推断和仿真辅助数据，实现对复杂软件系统抗辐射可靠性的合理预测。具体评估流程如下：

a） 数据准备：

1） 收集有限的真实辐射实验数据，包括但不限于典型辐射类型（如中子、质子、电磁波）、辐射强度、比特翻转位置、比特翻转方向以及对应的系统响应或故障记录；

2） 对原始数据进行筛选、清洗及格式统一，确保数据在统计分析中的一致性与可比性；

3） 在条件允许情况下，引入仿真数据作为辅助信息，用于补充样本覆盖范围并提供建模背景支撑。

b） 统计建模与推断：

1） 置信区间估计：基于小样本频率数据，构造故障率或可靠性指标的置信区间，给出合理的取值范围；

2） Bootstrap重采样：通过重复抽样构造大量伪样本集，估计参数分布及其方差，提高推断的稳健性；

3） 贝叶斯推断：在有限观测基础上引入先验知识（如器件失效率、历史试验经验），更新得到后验分布，从而提供带概率解释的区间推断。

c） 结果融合与验证：

1） 将统计推断结果与有限的仿真结果结合，提升评估的可信度；

2） 利用独立的小批量实验数据对估计结果进行交叉验证；

3） 在报告中不仅给出点估计，还需提供区间估计和不确定性说明。

d） 应用与扩展：

1） 在小样本条件下快速完成复杂软件系统抗辐射可靠性的评估；
2） 随着实验样本逐步增加，更新置信区间或后验分布，动态修正评估结果；
3） 可结合主动学习思想，选择最有价值的实验条件补充数据，提高评估效率与准确性。

11.2 等效评估

等效评估利用已有的大量仿真结果训练深度学习等效模型，将复杂的辐射与系统响应之间的关系转化为端到端预测器，从而在输入新的环境与设计参数时即可快速输出可靠性指标。具体等效评估流程如下：

a） 数据准备：
1） 设置多组辐射实验参数组合，包括但不限于典型辐射类型（如中子、质子、电磁波）、辐射强度、比特翻转位置、比特翻转方向以及工作模式等；
2） 通过辐射仿真平台获得对应的故障率、性能退化指标或系统输出特征；
3） 对数据进行清洗、标准化和特征提取，建立“参数—指标”的样本集。

b） 等效模型训练：
1） 选择深度学习模型（如卷积神经网络、多输入通道网络等），以多维参数作为输入，以故障率、性能退化指标或系统输出特征等作为输出；
2） 使用大规模仿真数据对模型进行训练，学习辐射条件与系统响应之间的映射关系；
3） 在训练过程中引入正则化和验证集，保证模型具备良好的泛化能力。

c） 模型校准与验证：
1） 使用少量真实辐射实验数据对训练好的模型进行校准，修正预测偏差；
2） 通过对比真实实验结果与模型输出，验证等效评估模型的准确性和稳定性。

d） 快速评估与应用：
1） 在模型确定后，当输入新的辐射环境条件或设计参数组合时，无需重复仿真，即可直接得到可靠性预测结果；
2） 在实际应用中结合不确定性分析与结果解释，确保输出结果具有工程可用性；
3） 随着新的真实实验数据积累，对等效模型进行持续更新和优化。

11.3 迁移评估

迁移学习的内涵在于将真实数据中更为准确、可靠的信息迁移到仿真数据域中，用以修正和校准仿真模型的偏差，使基于仿真生成的知识能够更贴近真实环境，从而提升评估的可信度和适用性。具体迁移评估流程如下：

a） 数据准备：
1） 收集大量辐射仿真数据，包括但不限于典型辐射类型（如中子、质子、电磁波）、辐射强度、比特翻转位置、比特翻转方向以及对应的系统响应或故障记录；
2） 获取少量真实辐射实验结果，用作可信基准，这些数据覆盖部分具有代表性的参数组合；
3） 对仿真数据和真实数据进行统一格式化与对齐，保证输入参数（如场强、频率、翻转位置、翻转方向）和输出指标（如失效率、崩溃率、SDC率）的一致性；
4） 将数据划分为“待修正域”（仿真）与“基准域”（真实），并准备验证与测试集。

b） 迁移模型训练：
1） 分析真实数据与仿真数据的分布差异，识别主要偏差来源；
2） 利用真实数据对仿真数据进行加权或校准，使仿真样本的统计特性向真实样本靠拢；
3） 构建迁移学习模型（如带有域自适应结构的深度神经网络），在大量仿真数据上训练模型，再通过少量真实数据微调、修正参数和特征映射；

4） 在训练过程中引入正则化与校准机制，确保迁移后的模型能更好地反映真实辐射环境下的可靠性结果。

c） 验证与应用：

1） 使用保留的真实实验数据对迁移模型进行验证，检验其预测结果与真实环境的吻合度；

2） 对比真实测量与预测结果，必要时进一步调整模型或校准策略；

3） 模型稳定后，可在输入新的辐射条件和设计参数时，快速给出贴近真实环境的评估结果。

参 考 文 献

[1] GB/T 34956－2017 大气辐射影响 航空电子设备单粒子效应防护设计指南
[2] GB/T 34955－2017 大气辐射影响 航空电子系统单粒子效应试验指南
[3] GB/T 40134-2021 航天系统电磁兼容性要求
[4] GB/Z 37150-2018 电磁兼容可靠性风险评估导则
[5] GB/T 41270.7－2022 航空电子过程管理 大气辐射影响 第 7 部分：航空电子产品设计中单粒子效应分析过程管理
[6] QJ 10005－2008 宇航用半导体器件重离子单粒子效应试验指南