|  |  |
| --- | --- |
| 标识：PT-RXXXX-TO-1.00 | 鉴定文件 |

XXXX

XXXX软件

鉴定测评大纲

册号：1/1 总页数：64

**中国科学院卫星软件评测中心**

XXXX年XX月XX日

XXXX软件

鉴定测评大纲

**拟制： XXXX 日期：XXXXXX**

**校对： XXXX 日期：XXXXXX**

**审核： 施敏华 日期：XXXXXX**

**批准： 韩 强 日期：XXXXXX**

|  |  |
| --- | --- |
| **有 效 性 声 明** | |
| 1．本中心严格按照安全有关保密要求开展测评工作，承担安全保密与知识产权保护有关的法律责任；  2．本测评大纲无授权签字人批准签字，大纲封面无中心印章无效；  3．本测评大纲未经中国科学院卫星软件评测中心书面批准，不得复制，任何未经允许的复制本，任何形式的残损本，不具备大纲原件的效力；  4．本大纲只适用于被测件介质相同版本的软件；  5．测评大纲版权归委托方和中国科学院卫星软件评测中心共有，其他任何单位和个人未经许可均无权使用本测评大纲，否则将保留对其追究法律责任的权利。 | |
| 测试机构名称 | 中国科学院卫星软件评测中心 |
| 测试机构地址 | 上海市浦东新区雪洋路1号3楼 |

文件状态表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 日期 | 更改摘要 | 修改章节 | 备注 |
| V0.10 | XXXXXX | 创建文档 | / | 内审版本 |
| V1.00 | XXXXXX | 1、修改调整软硬件环境 | 1、5.2章节 | 内部评审修改 |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[1 范围 3](#_Toc196313699)

[1.1 标识 3](#_Toc196313700)

[1.2 文档概述 3](#_Toc196313701)

[1.3 测评依据 3](#_Toc196313702)

[1.3.1 测评任务来源 3](#_Toc196313703)

[1.3.2 依据文件 4](#_Toc196313704)

[2 测评性质 5](#_Toc196313705)

[3 测评目的 5](#_Toc196313706)

[4 测评时间和地点 5](#_Toc196313707)

[5 测评对象及环境 7](#_Toc196313708)

[5.1 测评对象 7](#_Toc196313709)

[5.1.1 测评对象基本信息 7](#_Toc196313710)

[5.1.2 软件概述 8](#_Toc196313711)

[5.2 测评环境 10](#_Toc196313712)

[5.2.1 静态测试环境 10](#_Toc196313713)

[5.2.2 动态测试环境 11](#_Toc196313714)

[6 测评要求、内容及方法 13](#_Toc196313715)

[6.1 测评总体要求 13](#_Toc196313716)

[6.1.1 测试级别和类型 13](#_Toc196313717)

[6.1.2 测试策略和方法 14](#_Toc196313718)

[6.2 测试项及方法 15](#_Toc196313719)

[6.2.1 文档审查 15](#_Toc196313720)

[6.2.2 静态分析 16](#_Toc196313721)

[6.2.3 代码审查 17](#_Toc196313722)

[6.2.4 功能测试 18](#_Toc196313723)

[6.2.5 接口测试 22](#_Toc196313724)

[6.2.6 摸底测试 23](#_Toc196313725)

[6.3 测评内容充分性及方法有效性分析 24](#_Toc196313726)

[6.4 评价内容及方法 24](#_Toc196313727)

[6.4.1 软件需求符合性 24](#_Toc196313728)

[6.4.2 软件指标符合性 24](#_Toc196313729)

[6.4.3 软件质量评价 24](#_Toc196313730)

[6.5 问题类别及等级 25](#_Toc196313731)

[6.5.1 问题类型 25](#_Toc196313732)

[6.5.2 问题严重性等级 25](#_Toc196313733)

[6.5.3 问题处理方法 26](#_Toc196313734)

[6.6 测评通过准则 27](#_Toc196313735)

[6.7 测评数据采信 27](#_Toc196313736)

[7 测评度量数据及采集要求 27](#_Toc196313737)

[8 测评暂停、恢复与终止 27](#_Toc196313738)

[9 测评组织及任务分工 28](#_Toc196313739)

[10 测评保障 28](#_Toc196313740)

[10.1 测评条件保障 28](#_Toc196313741)

[10.2 配置管理 29](#_Toc196313742)

[10.3 质量保证 30](#_Toc196313743)

[10.3.1 质量保证要求 30](#_Toc196313744)

[10.3.2 质量保证计划 30](#_Toc196313745)

[10.4 评审与控制 31](#_Toc196313746)

[10.4.1 设计评审 31](#_Toc196313747)

[10.4.2 过程控制 31](#_Toc196313748)

[10.4.3 文档控制 31](#_Toc196313749)

[10.4.4 人员控制 32](#_Toc196313750)

[10.5 测评风险分析 32](#_Toc196313751)

[10.6 测评分包 33](#_Toc196313752)

[11 测评安全与保密 33](#_Toc196313753)

[12 有关问题的说明 33](#_Toc196313754)

[附录A 文档审查单 34](#_Toc196313755)

[A.1 文档齐套性查单 34](#_Toc196313756)

[A.2 软件需求规格说明审查单 34](#_Toc196313757)

[A.3 软件设计文档审查单 36](#_Toc196313758)

[附录B 代码审查单 38](#_Toc196313759)

[B.1 C语言代码审查单 38](#_Toc196313760)

[附录C 静态分析审查单 42](#_Toc196313761)

[C.1 代码质量度量分析表单 42](#_Toc196313762)

[C.2 代码编码规则表 43](#_Toc196313763)

[C.3 控制流分析表单 50](#_Toc196313764)

[C.4 数据流分析表单 51](#_Toc196313765)

[附录D 软件需求与测试需求对照表 52](#_Toc196313766)

[D.1 测试需求与研制总要求（或技术协议）覆盖情况表 52](#_Toc196313767)

[D.2 测试需求与需求规格说明覆盖情况表 52](#_Toc196313768)

XXXX软件鉴定测评大纲

# 范围

## 标识

1）文档标识号：PT-RXXXX-TO-1.00

2）标题：XXXX软件鉴定测评大纲

3）本文档适用的软件：XXXX软件-R/XX03-XXX/02-VX.X.XX

## 文档概述

本大纲描述了XXXX软件测评的测试目的、测试策略、测试内容、测试技术与测试方法、测试结束和终止条件、评价方法与结论、测试环境要求、测试进度、人员安排和风险分析等内容，是XXXX软件鉴定测评的依据。

## 测评依据

### 测评任务来源

1）委托单位与联系方式

委托单位名称：XXXX试验XX处

委托单位地址：XXXX

联系人：XXXX

联系电话：13888888888

2）承研单位与联系方式

承研单位名称：XXX研究所

承研单位地址：XXX七号

联系人：XXXX

联系电话：13888888888

3）测评机构与联系方式

测评机构名称：中国科学院卫星软件测评中心

承研单位地址：上海市海科路99号

联系人：XXXX

联系电话：13888888888

### 依据文件

#### 管理文件

测评工作依据的管理文件见下表。

表1‑1依据的管理文件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 文档名称 | 标识/版本 | 发布日期 | 来源 |
|  | 关于改进加强军用软件产品试验鉴定工作的有关要求（试行） | 军定〔2022〕9号 | 2022-03-22 | 国务院、中央军委军工产品定性委员会 |
|  | 军用软件测评实验室测评过程和技术能力要求 | 〔2005〕装电字第324号 | 2005-12 | 总装备部电子信息基础部 |
|  | 军用软件试验鉴定通用要求 | TE-BTCG-002-2021 | 2021-09-10 | 中央军委装备发展部 |
|  | 军用软件测试指南 | TE-BTCG-003-2021 | 2021-09 | 中央军委装备发展部 |
|  | 军用软件鉴定测评指南 | TE-BTCG-004-2021 | 2021-09 | 中央军委装备发展部 |
|  | 军用软件鉴定测评大纲和报告 | TE-BTCG-007-2021 | 2021-09 | 中央军委装备发展部 |
|  | 军用软件开发文档通用要求 | GJB 438C-2021 | 2022-03-01 | 中央军委装备发展部 |
|  | C/C++语言编程安全子集 | GJB 8114-2013 | 2013-04-11 | 国防科学技术工业委员会 |
|  | 军用软件开发通用要求 | GJB 2786A-2009 | 2009-08-20 | 原总装备部 |

#### 顶层技术文件

测评工作依据的顶层技术文件见下表。

表1‑2依据的顶层技术文件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 文档名称 | 标识/版本 | 发布日期 | 来源 |
|  | DMM-XXX研制任务书 | XXX-XXXX | 2022-06-14 | 中国航天科工集团X院X部 |
|  | XXX软件研制技术协议 | XXX-XXXX | 2022-06-14 | 中国电子科技集团公司第XX研究所 |
|  | XXX试验总案 | XXX-XXXX | 2022-06-14 | XXX试验监管局 |
|  | XXX研制总要求 | XXX-XXXX | 2022-06-14 | XXX |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### 被测软件文档

测评工作依据的被测软件文档见下表。

表1‑3依据的被测软件文档

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 文档名称 | 标识/版本 | 发布日期 | 来源 |
|  | 需求规格说明 | R/XX03-XXX/02\_RX XX03-XXX-VX.X.00 | 2025-04-17 | XXX研究所 |

# 测评性质

本次测评任务性质为软件鉴定测评。

# 测评目的

本次测评目的为发现并纠正软件问题缺陷，考核XXXX软件功能、性能指标是否满足规定的要求，对软件边界性能及性能底数进行摸底，为装备鉴定和列装定型提供依据。

# 测评时间和地点

测评时间周期：XX年X月至XX年X月。

测评地点：静态测试在上海市中国科学院软件测评中心、动态测试在XXX研究所

测评主要时间节点及地点见下表。

表4‑1测评时间和地点

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评工作 | 起止时间 | 地点 |
|  | 被测件初次接收 | XXXX~XXXX | 中国科学院卫星软件评测中心 |
|  | 测评大纲编制 | XXXX~XXXX | 中国科学院卫星软件评测中心 |
|  | 测评大纲评审 | T（天）（T为测评大纲评审时间） | / |
|  | 测评设计与实现 | XXXX~XXXX | 中国科学院卫星软件评测中心 |
|  | 测评执行 | T0~T0+21（天）（T0为测试环境就绪事件） | XXX研究所实验室 |
|  | 测评总结 | T1~T1+5（天）（T1为所有版本测试完成时刻） | 中国科学院卫星软件评测中心 |
|  | 测评总结评审 | T2（T2为测评总结评审时刻） | / |

# 测评对象及环境

## 测评对象

### 测评对象基本信息

本次测评对象基本信息见下表。

表5‑1被测软件基本信息表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 软件所在子系统/设备名称 | 软件名称 | 软件类型 | 重要/安全等级 | 运行环境 | 开发环境 | 编程语言 | 版本 | 代码规模  （软件规模/代码行） | 接收日期 | 研制单位 |
|  | XXXX软件 | XXXX软件 | 新研 | C | XXXX | XXXX | C  C++ | X.X.XX | XXXX | XX-X-X | XXX研究所 |

### 软件概述

XX03-XXXXXX单元用于某型产品，主要由传声器阵列和主机等组成。

XX03-XXXXXXX主机软件包括XXXXX软件和XXXX软件，其中声探测信息交互软件主要基于XXXX（国产）与XXXX（国产），完成与XX控制系统的信息交互功能。

XXXX软件分两个部分。一是XXX模块，二是XXXX模块，模块间通过内部网口进行信息交互。功能模块框图如下所示。

图5-1模块组成图

#### 软件主要功能和性能指标

XXXX软件主要功能要求如下表所示。

表5‑2XXXX软件功能指标覆盖表

|  |  |  |
| --- | --- | --- |
| 需求章节号 | 功能指标 | 测评覆盖情况 |
| 《需求规格说明》3.2.2.1.1-XXX功能 | XXX模块主要实现以下功能：  1）XXXXXX | XXXXX |

XXXX软件主要性能要求如下表所示。

表5‑3XXXX性能指标覆盖表

|  |  |  |
| --- | --- | --- |
| 需求章节号 | 性能指标 | 测评覆盖情况 |
| 《需求规格说明》3.2.2.2.6-XXXX模块 | XXXX | XXXX |

XXXX软件测评摸底指标清单如下表所示。

表5‑4XXXX软件摸底指标清单

|  |  |  |  |
| --- | --- | --- | --- |
| 需求来源 | 描述 | 测试项名称 | 测试项标识 |
| 隐含需求 | 测试绝对时统和相对时统差距最大到多大时、最小到多小相差时，记录下差值 | 切换相对时统误差摸底测试 | XQ\_MD\_XDST |

#### 软件接口说明

XXXX软件的外部接口主要包含与XXXX软件接口。XXXX软件软件外部接口示意图如下图所示。

图5-2XXXX接口示意图

XXXX软件外部接口信息见下表所示。

表5‑2XXXX软件接口信息表

| 序号 | 接口名称 | 接口标识 | 接口描述 | 来源 | 目的地 | 接口类型 |
| --- | --- | --- | --- | --- | --- | --- |
|  | 与XXXX接口 | INI1\_1 | XXXXX | XXX软件 | XXXX模块 | 串口 |

## 测评环境

### 静态测试环境

#### 环境描述

本次测试的静态环境包括：静态测试工具、测试计算机、被测软件源代码和被测软件文档。测试工作安装在测试计算机上，被测软件源代码拷贝到计算机进行静态分析。

#### 软件项

此次静态测试环境使用的软件项见下表所示。

表5‑6静态测试环境软件项

| 序号 | 软件项名称 | 版本 | 用途 | 提供单位 |
| --- | --- | --- | --- | --- |
|  | XXX软件 | 4.A.00 | 被测软件源代码 | XXX研究所 |
|  | Klocwork | V2018 | 用于运行错误检测 | 中国科学院卫星软件测评中心 |
|  | TestBed | V9.4 | 用于静态分析 |
|  | Microsoft Office | 2016 | 文档阅读、编辑工具 |
|  |  |  |  |  |

#### 硬件和固件项

此次静态测试环境使用的硬件和固件项见下表所示。

表5‑7静态测试环境硬件和固件项

| 序号 | 硬件或固件项名称 | 设备编号 | 用途 | 配置 | 提供单位 |
| --- | --- | --- | --- | --- | --- |
|  | 测试PC | TY2023030023 | 运行辅助软件，用于静态测试和代码审查 | CPU:13th Gen Intel(R) Core(TM) i5-13500H 2.60GHz  内存：16G  硬盘：1T  操作系统：Windows 10(64) | 中国科学院卫星软件测评中心 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

#### 静态测试场所

中国科学院卫星软件测评中心。

### 动态测试环境

#### 环境描述

测试环境由XX单元主机（XX软件、XX软件MCU模块）、XX通信机（信息交互软件通信模块）、XXX、XXX测试系统（XX）、交换机、调试计算机1、调试计算机2、调试计算机3、仿真器、调试显示屏、主机电池组成。其中XXX，XXX通信机，调试计算机通过网线与交换相连进行通信。测试环境如下图所示。

图5-3XXX软件动态测试环境图

#### 软件项

XX软件动态测试环境使用的软件项见下表所示。

表5‑8动态测试环境软件项

| 序号 | 软件项名称 | 版本 | 用途 | 提供单位 | 部署位置 |
| --- | --- | --- | --- | --- | --- |
|  | XX软件 | VXX.X | 被测软件 | 某研究所 | XX主机 |
|  | XX软件 | VXX.X | 陪测软件，用于XX | XX研究所 | XX主机 |
|  |  |  |  |  |  |

#### 硬件和固件项

动态测试环境使用的硬件和固件项见下表所示。

表5‑9动态测试环境硬件和固件项

| 序号 | 硬件或固件项名称 | 设备编号 | 用途 | 配置 | 状态 | 提供单位 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | XX主机 | 编号：2001002 | 实装运行环境，运行信息交换软件的MCU模块 | GDXXX国产芯片 | 受控被测件 | XX研究所 |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |

#### 测评场所

XXXX软件动态测试在XXXX实验室进行，测评场所的安全保密工作由XXXX研究所负责。

#### 测评数据

本次测评所需的测评数据见下表。

表5‑10测评数据

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 数据描述 | 性质 | 规格 | 数量 | 密级 | 提供单位 |
| 1 | XXX信号数据 | 实时采集 | XXX环境 | 多于20组 | MM | XXX研究所 |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |

#### 环境差异性分析

被测软件运行在实装环境进行测试，正常功能测试和接口测试均使用真实设备进行测试，信号输入端使用XXX采集XXX数据，接口异常使用XXX模拟错误，经过分析对本次测试结果无影响。环境差异影响分析表见下表所示。

表5‑11测评环境差异影响分析表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 真实环境 | 测试环境 | 环境差异及对测评结果影响 |
| 1 | XX系统 | XX工具 | XX和XX等效，故对测试结果无影响 |
| 2 |  |  |  |

# 测评要求、内容及方法

## 测评总体要求

### 测试级别和类型

本次测评测试级别为配置项测试。本配置项测试安全等级为XX，按照《军用软件鉴定测评指南》要求，配置项测试的测试类型要求如下表所示。

表6‑1不同等级软件的测试类型要求以及选取类型

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试类别 | 测试类型 | 功能指标 | | | 选取情况 |
| 关键A | 重要B | 一般C/D |
| 文档类 | 文档审查 | ● | ● | ● | √ |
| 代码类 | 代码审查 | ● | ● | ○ | √ |
| 代码走查 | ○ | ○ | - | - |
| 静态分析 | ● | ● | ● | √ |
| 逻辑测试 | ○ | ○ | - | - |
| 数据类 | 数据审查 | ○ | ○ | ○ | - |
| 数据处理测试 | ○ | ○ | ○ | - |
| 功能类 | 功能测试 | ● | ● | ● | √ |
| 边界测试 | ● | ● | ● | √ |
| 恢复性测试 | ● | ○ | ○ | √ |
| 安装性测试 | ○ | ○ | ○ | - |
| 性能类 | 性能测试 | ● | ● | ● | √ |
| 余量测试 | ● | ● | ○ | √ |
| 容量测试 | ○ | ○ | ○ | - |
| 强度测试 | ● | ○ | - | √ |
| 接口类 | 接口测试 | ● | ● | ● | √ |
| 人机交互界面测试 | ○ | ○ | ○ | √ |
| 专项类 | 安全性测试 | ● | ● | ○ | √ |
| 可靠性测试 | ○ | - | - | - |
| 兼容性测试 | ○ | ○ | ○ | - |
| 互操作性测试 | ○ | ○ | ○ | - |

注：●必须开展，○根据软件特点视情况要求开展，-不开展。√为选取的测试类型

对软件测评中未选取测试类型的情况说明如下表。

表6‑2未选取测试类型情况说明表

|  |  |
| --- | --- |
| 测试类型 | 测评覆盖情况 |
| 代码走查 | 该软件重要级别为一般，故不开展该测试类型测试 |
| 数据审查 | 因软件固定配置参数要求，故不开展相关测试类型测试 |
| 逻辑测试 | 该软件重要级别为一般，故不开展相关测试类型测试 |
| 安装性测试 | 软件为嵌入式软件，故不开展相关测试类型测试 |
| 容量测试 | 软件需求规格说明中无容量要求，故不开展相关测试类型测试 |
| 兼容性测试 | 软件因为没有兼容性测试需求，故不开展相关测试类型测试 |
| 互操作性测试 | 软件需求规格说明中无容量要求，故不开展相关测试类型测试 |

### 测试策略和方法

#### 测试策略

依据《军用软件测试指南》、《军用软件鉴定测评指南》、软件任务书和软件需求规格说明等文档，结合XX软件特点和承研单位提供的测试环境，制定以下测评策略：

1）对XX软件进行配置项级别测试

2）先开展静态测试，待发现问题整改后开展动态测试

3）对测试过程中发生的软件更改和版本升级要依据软件开发方提交的软件更改单进行更改确认，并对软件的更改进行测试的影响域分析，开展回归测试

4）测试过程中存在有争议的问题，应组织研制单位、软件测评机构、软件总体单位等相关方确认进行确认

5）XXX无法动态测试验证，借助插桩等手段验证

6）本次摸边探底指标选择如下：XXX最大时间、XXX最小距离

#### 测试方法

表6‑3配置项测试类型和测试方法

| 测试类型  名称 | 测试类型标识 | 测试内容及方法描述 |
| --- | --- | --- |
| 文档审查 | DC | 通过人工审查的方式，依据《军用软件开发文档通用要求》，对研制方提交的软件需求规格说明、设计文档进行审查。文档审查依据文档检查单 |
| 静态分析 | SA | 利用静态分析工具辅助进行控制流分析、数据流分析、接口特性分析和表达式分析，验证软件质量度量和编码规则是否满足标准要求 |
| 代码审查 | CR | 按照经过评审的代码审查单，使用测试工具Klocwork和人工审查相结合的方式，对软件进行代码和设计的一致性、代码编程规范性检查 |
| 功能测试 | SU | 功能测试根据被测软件的功能特点，  用正常值的等价类输入数据值测试；  b）用非正常值的等价类输入数据值测试；  c）进行每个功能的合法边界值和非法边界值输入的测试；  d）用一系列真实的数据类型和数据值运行，测试超负荷、饱和及其他“最坏情况”的结果；  e）对控制流程的正确性、合理性等进行验证；  f）对用户接口正常和异常数据输入的测试。 |
| 接口测试 | IO | 对配置项接口测试主要测试配置项软件的对外接口，对子系统接口进行测试主要测试子系统的对外接口；  1、测试输出的数据格式是否满足通信协议的要求；  2、对传输发生异常的数据，软件是否有相应的容错机制。 |

## 测试项及方法

### 文档审查

#### 文档审查

表1‑2文档审查测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 文档审查 | 测试项标识 | XQ\_DC\_WDSC | 优先级 | 高 |
| 追踪关系 | 隐含需求 | | | | |
| 需求描述 | 依据相关要求，逐项检查被测文档的齐套性、完整性、一致性和准确性是否满足要求 | | | | |
| 测试手段 | 静态测试 | | | | |
| 测试项描述 | 本次文档审查包括的内容如下：  1）软件研制总结报告  2）软件开发计划  3）软件运行方案说明  4）软件接口需求规格说明  5）软件系统设计说明  6）软件接口设计说明  7）软件需求规格说明  8）软件配置项设计说明  9）软件测试说明  10）软件测试报告  11）产品规格说明  12）软件版本说明  13）软件用户手册  14）固件保障手册 | | | | |
| 测试方法 | **1.文档审查（XQ\_DC\_WDSC\_SU01）**  1）根据文档审查表人工逐项检查，检查此项目文档的齐套性、完整性、规范性：  1）使用人工审查方法，按照附录A中文档齐套性审查单检查需求类、设计类、用户类、测试类文档是否齐套；  2）使用人工审查方法，按照附录A中需求规格说明审查单对软件需求规格说明逐项检查；  3）使用人工审查方法，按照附录A中软件设计文档审查单逐项检查。 | | | | |
| 充分性要求 | 按照审查单审查文档的齐套性、完整性、一致性、准确性。 | | | | |
| 通过准则 | 1）被测软件文档种类齐全，内容完整，描述准确，格式规范；  2）需求文档内容完整，描述准确，格式规范，文档文文一致、文实相符；  3）设计说明文档内容完整，描述准确，格式规范，文档文文一致、文实相符。 | | | | |

### 静态分析

#### 静态分析

表1‑2静态分析测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 静态分析 | 测试项标识 | XQ\_SA\_JTFX | 优先级 | 中 |
| 追踪关系 | 隐含需求 | | | | |
| 需求描述 | 依据相关的要求，利用静态分析工具对被测软件全部源程序进行控制流分析、数据流分析进行分析，并统计软件质量度量信息，给出软件源代码检查结果 | | | | |
| 测试手段 | 静态测试 | | | | |
| 测试项描述 | 对被测软件全部源程序进行静态分析，对控制流、数据流进行分析，验证软件是否满足控制流和数据流要求，并依据质量特性需求统计质量度量信息 | | | | |
| 测试方法 | **1.静态分析（XQ\_SA\_JTFX\_SU01）**  1）根据静态分析的审查项和技术要求以及被测软件质量特性需求，编制检查单。使用静态分析工具Testbed和klocwork进行静态分析，对程序进行检查：  1）使用静态分析工具统计软件质量度量信息；  2）使用静态分析工具对软件进行规则检查；  3）使用静态分析工具结合人工分析对控制流和数据流进行分析。 | | | | |
| 充分性要求 | 1）对软件全部源代码进行静态分析；  2）对度量指标不满足指标要求的模块，应进行专项代码审查；  3）按照控制流和数据流分析表单，对软件的控制流和数据流进行分析。 | | | | |
| 通过准则 | 1） 完成要求的源代码分析，得到软件质量度量信息；  2） 软件总注释率不小于20%（注释行数/代码行数\*100%）；  3） 无违反控制流和数据流分析检查要求的情况。 | | | | |

### 代码审查

#### 代码审查

表1‑2代码审查测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 代码审查 | 测试项标识 | XQ\_CR\_DMSC | 优先级 | 中 |
| 追踪关系 | 隐含需求 | | | | |
| 需求描述 | 依据相关要求及软件文档开展针对软件程序代码的代码审查 | | | | |
| 测试手段 | 静态测试 | | | | |
| 测试项描述 | 通过人工审查及借助klocwork、Testbed工具辅助分析的方式开展代码审查，审查代码和设计的一致性、代码执行标准的情况、代码逻辑表达的正确性、代码结构的合理性以及代码的可读性。人工审查中发现的问题，审查人员应及时记录。 | | | | |
| 测试方法 | **1.代码审查（XQ\_CR\_DMSC\_SU01）**  1）使用klocwork、testbed工具根据本大纲附录B中的代码审查单对代码审查范围内的源代码开展四个方面的审查，人工对所选模块进行如下四个方面的审查：  1）编程准则检查：依据编程准则的要求，对程序的编码与编程准则进行符合性检查；  2）代码流程审查：审查程序代码的条件判别、控制流程、数据处理等满足设计要求；  3）软件结构审查：依据设计文档，审查程序代码的结构设计的合理性，包括程序结构设计和数据结构设计；  4）需求实现审查：依据需求文档及其他相关资料，审查程序代码的需求层的功能实现是否正确。 | | | | |
| 充分性要求 | 根据代码审查单的审查项，工具审查完成全部代码的审查，人工审查完成关键模块的审查，审查中发现的问题均得到有效处理。 | | | | |
| 通过准则 | 完成要求的源代码审查，软件没有违反代码审查单的要求；  代码与设计需求一致，满足编码规则强制项的要求。 | | | | |

### 功能测试

#### 探测显示功能测试

表1‑2探测显示功能测试测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 探测显示功能测试 | 测试项标识 | XQ\_SU\_TCXS | 优先级 | 高 |
| 追踪关系 | 《需求规格说明》-3.2.2.1.1-探测显示功能 | | | | |
| 需求描述 | 探测显示功能模块主要实现以下功能：  1）开机显示：显示设备名称及生产厂家；  输入DSP握手信息，输出界面显示，显示设备名称以及生产厂家。  2）探测结果：显示目标批号、方向、类型；  输入探测结果信息，输出界面显示，显示目标批次（1,2,3,4,5）、目标方位（000.0）、目标类型（0000）。  3）环境噪声等级：显示环境噪声等级；  输入环境噪声等级信息，输出界面显示，显示优、良、中、差。  4）系统时间：显示系统时间。  输入时间信息，输出界面显示，显示格式为（时：分：秒） | | | | |
| 测试手段 | 动态测试 | | | | |
| 测试项描述 | 动态测试环境下，设备上电启动，观察开机显示界面是否正确；通过信号处理软件发送正常或者异常探测结果、环境噪声等级、验证是否能够正确显示；验证是否能够正确显示系统时间 | | | | |
| 测试方法 | **1.开机显示（XQ\_SU\_TCXS\_SU01）**  1）设备上电开机后，检查设备界面是否显示设备名称以及生产厂家  2）确认显示的生产厂家是否为声探测单元设备的厂家  3）确认显示的设备名称是否正确  **2.探测结果显示（XQ\_SU\_TCXS\_SU02）**  1）通过信号处理软件仿真器调整输出给主机控制模块异常的批次信息（6个、7个），检查显示屏显示内容是否正确  2）在动态测试环境下，通过目标定向识别测试系统给声探测单元发送测试数据，分别发送目标类型为：0（未识别）、02（固定翼）、03（四旋翼和六旋翼），查看显示屏是否正确显示0（未识别）、02（固定翼）、03（四旋翼和六旋翼）的目标类型，所属类型均和输入对应  3）在非探测页面的其他页面下，按下“探测”按钮，查看显示屏是否跳转到探测结果显示界面  4）通过信号处理软件仿真器修改输出给主机控制模块异常的方向信息（0xFFFFFFFFFF），查看显示屏内容是否正确  5）设备正常启动后，查看设备在显示完设备名称和生产厂家后是否自动跳转到探测结果显示页面  6）在动态测试环境下，通过16通道声探测仪输入数据，通过模拟方位30°、60°、90°、120°、150°、180°、210°、240°、270°、300°、330°，查看显示屏显示的方位是否和模拟的方位误差不超过4%  7）在动态测试环境下，通过目标定向识别测试系统不断更换声音数据，查看显示屏显示的批号、方向、类型等信息是否会更新，并且更新时间为立即  8）通过信号处理软件仿真器修改输出给主机控制模块异常的目标类型（不包含0、150、151、152的其他数值），查看显示屏内容是否显示正确  9）在动态测试环境下，通过目标定向识别测试系统给声探测单元发送测试数据，分别发送1~5批次可正常识别的目标，查看显示界面显示的批次1~5是否排列正确 | | | | |
| 充分性要求 | 测试用例覆盖开机显示子项要求的全部内容。  所有用例执行完毕，对于未执行的用例说明未执行原因。 | | | | |
| 通过准则 | **1.开机显示（XQ\_SU\_TCXS\_SU01）**  1）设备界面显示设备名称、生产厂家，清晰可读  2）显示的生产厂家为“中国电子科技集团公司第三研究所”  3）显示的设备名称是“声探测单元主机”  **2.探测结果显示（XQ\_SU\_TCXS\_SU02）**  1）显示屏不显示异常的批次，显示数量最多到5个  2）查看显示屏正确显示0、150、151、152的目标类型  3）按下“探测”按钮，查看显示屏会立即跳转探测结果显示界面  4）显示屏不显示异常的方位信息  5）显示完设备名称和生产厂家后自动跳转到探测结果显示页面  6）典型数据输入情况下，方位数据显示正确和实际一致  7）显示屏显示的批号、方向、类型等信息会立即更新  8）显示屏可显示在数值范围内（10Bytes）的数量也可以显示错误信息  9）显示屏可显示1、2、3、4、5批次数量 | | | | |

#### 数据储存时间性能

表1‑2数据储存时间性能测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 数据储存时间性能 | 测试项标识 | XQ\_SU\_CCSJ | 优先级 | 高 |
| 追踪关系 | 《需求规格说明》-3.2.2.2.6-数据记录功能模块 | | | | |
| 需求描述 | 声学探测单元的决策信息、控制信息、状态信息等本地存储，数据存储时间要求：不小于一个月 | | | | |
| 测试手段 | 动态测试 | | | | |
| 测试项描述 | 通过检查存储的数据记录时间验证该性能指标的符合性，如果无法检查储存数据时间，采用预估测试方法，计算最大每日数据记录数据，并考察储存策略，判断是否在31日内数据能否达到数据储存上限或删除阈值 | | | | |
| 测试方法 | **1.数据存储时间性能测试（XQ\_SU\_CCSJ\_SU01）**  1）如果无法检查储存数据时间，采用等效性评估方法，计算最大每日数据记录数据，并考察储存策略，判断是否在31日内数据能否达到数据储存上限或删除阈值  2）如果为文件形式，查看历史记录数据是否达到储存一个月时间  3）测试决策信息、控制信息、状态信息等本地存储的采用储存形式 | | | | |
| 充分性要求 | 测试用例覆盖数据存储时间性能测试子项要求的全部内容。  所有用例执行完毕，对于未执行的用例说明未执行原因。 | | | | |
| 通过准则 | **1.数据存储时间性能测试（XQ\_SU\_CCSJ\_SU01）**  1）决策信息、控制信息、状态信息等本地存储能够达到1个月时间  2）文件记录时间相差1个月  3）决策信息、控制信息、状态信息等本地存储能够达到1个月时间 | | | | |

### 接口测试

#### 与声探测信号处理软件接口

表1‑2与声探测信号处理软件接口测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 与声探测信号处理软件接口 | 测试项标识 | XQ\_IO\_INT1 | 优先级 | 高 |
| 追踪关系 | 《需求规格说明》-3.3-与声探测信号处理软件接口 | | | | |
| 需求描述 | 处理和声探测信号处理软件接口 | | | | |
| 测试手段 | 动态测试 | | | | |
| 测试项描述 | 在实装测试环境下，使用仿真器查看是否能够接收到探测结果，环境噪声分级以及通道的自检结果，且正常发送的环境温度和自检指令，验证与声探测信号处理软件的串口通信是否正常 | | | | |
| 测试方法 | **1.接收正常数据（XQ\_IO\_INT1\_SU01）**  1）使用信息处理软件向信息交互软件发送探测结果报文，通过仿真器查看是否收到正确的探测结果报文；或者通过OLED显示屏的探测界面中，检查显示界面是否显示目标批号、方向、类型等探测结果信息  2）使用信息处理软件向信息交互软件发送环境噪声分级（优、良、差）报文，通过仿真器查看是否收到正确的环境噪声分级报文；或者通过OLED显示屏的探测界面中，检查显示的环境噪声分级是否与发送的一致  3）检查接收到的探测结果报文格式是否与协议一致  4）检查接收到的环境噪声分级报文格式是否与协议一致 | | | | |
| 充分性要求 | 测试用例覆盖接收正常数据子项要求的全部内容。  所有用例执行完毕，对于未执行的用例说明未执行原因。 | | | | |
| 通过准则 | **1.接收正常数据（XQ\_IO\_INT1\_SU01）**  1）收到正确的探测结果报文；通过OLED显示屏的探测界面中，显示界面显示目标批号、方向、类型等探测结果信息  2）收到正确的自检结果报文；通过OLED显示屏的自检界面中，显示的自检结果是发送信息一致，收到正确报文；通过OLED显示屏的探测界面中，显示的环境噪声分级与发送的一致  3）接收到的探测结果报文格式与协议一致  4）接收到的环境噪声分级报文格式与协议一致 | | | | |

### 摸底测试

#### 切换相对时统误差摸底测试

表1‑2切换相对时统误差摸底测试测试项

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试项名称 | 切换相对时统误差摸底测试 | 测试项标识 | XQ\_MD\_XDST | 优先级 | 高 |
| 追踪关系 | 隐含需求 | | | | |
| 需求描述 | 声探测单元主机默认使用绝对时统，当绝对时统和相对时统（麒麟系统时间）差值大于2s或小于200ms时，主机会切换为相对时统 | | | | |
| 测试手段 | 动态测试 | | | | |
| 测试项描述 | 当声探测单元主机连接声探测信息交互软件的通信管理模块，声探测单元主机默认使用绝对时统，手动设置通信模块相对时统（麒麟系统时间），不断设置系统时间和绝对时统相差逐步增大和缩小，测试绝对时统和相对时统差距最大到多大时、最小到多小相差时，记录下差值 | | | | |
| 测试方法 | **1.切换相对时统最大时差（XQ\_MD\_XDST\_SU01）**  1）在动态测试环境下，声探测单元主机正确连接声探测信息交互软件通信模块，并和模拟的网络调试助手正确连接，通过发送绝对时统信息，检查显示屏是否显示为使用的绝对时统  2）不断增大绝对时统和相对时统差值，检查在时间差值为多少时切换为相对时统，注意差值时等待5s以上确认当前时统状态  **2.切换相对时统最小时差（XQ\_MD\_XDST\_SU02）**  1）不断减小绝对时统和相对时统差值，检查在时间差值为多少时切换为相对时统 | | | | |
| 充分性要求 | 测试用例覆盖切换相对时统最大时差、切换相对时统最小时差子项要求的全部内容。  所有用例执行完毕，对于未执行的用例说明未执行原因。 | | | | |
| 通过准则 | **1.切换相对时统最大时差（XQ\_MD\_XDST\_SU01）**  1）在动态测试环境下，声探测单元主机正确连接声探测信息交互软件通信模块，并和模拟的网络调试助手正确连接，通过发送绝对时统信息，检查显示屏是否显示为使用的绝对时统  2）不断增大绝对时统和相对时统差值，检查在时间差值为多少时切换为相对时统，注意差值时等待5s以上确认当前时统状态  **2.切换相对时统最小时差（XQ\_MD\_XDST\_SU02）**  1）当绝对时统和相对时统时间差减小达到一定值后声探测单元切换为相对时统，已记录该时间差的值 | | | | |

## 测评内容充分性及方法有效性分析

XXXX软件软件测试共6种测试类型，其中静态分析1项、代码审查1项、文档审查1项、功能测试2项、摸底测试1项、接口测试1项。实现测试需求对软件需求的100%覆盖，具体详见附录D追踪表内容。

按照《军用软件测试指南》、《军用软件鉴定测评指南》等相关规定要求，进行测试策划，测试方法适合、有效。

## 评价内容及方法

### 软件需求符合性

从以下两方面评价软件需求符合性：

1）软件是否实现了软件任务书中规定的相关功能、性能需求；

2） 软件是否实现了软件需求规格说明中规定的相关功能、性能需求。

### 软件指标符合性

从以下两方面评价软件指标符合性：

1）软件是否实现了任务书及需求中规定的全部软件相关要求；

2） 软件性能是否满足相关要求。

### 软件质量评价

从以下几个方面评价软件质量：

1） 软件编码质量是否满足要求，用代码的质量度量元统计度量编码质量，包括：

a）软件总注释率不小于20%；

b）模块的平均规模不大于200行；

c）模块的平均圈复杂度不大于10；

d）模块的平均扇出数不大于7。

2） 统计软件首轮测试缺陷率及每轮回归测试缺陷率。

3） 软件文档种类是否齐套、内容是否完整、描述是否准确、格式是否规范及文档是否文文一致、文实相符。

4） 测试中发现问题的修改处理情况，对遗留问题的影响分析。

## 问题类别及等级

### 问题类型

根据TE-BTCG-003-2021《军用软件测试指南》，本次测试对软件问题类型作如下分类：

1）需求问题：用户需求、系统需求或软件需求问题；

2） 设计问题：系统设计或软件设计问题；

3） 文档问题：文档描述问题；

4） 编码问题：代码实现问题；

5） 数据问题：数据规格及内容问题；

6） 其他问题：上述问题之外的问题。

### 问题严重性等级

根据TE-BTCG-003-2021《军用软件测试指南》，软件问题按照重要度等级划分为以下等级，具体说明如下：

1） 重大问题：软件问题导致程序无法继续运行、丧失主要功能或造成重大损失的，视为重大问题：

a）导致系统死机、崩溃或异常退出；

b）主要功能未实现或实现错误；

c）造成人员、装备、环境等重大损失；

d）重要数据丢失，且很难恢复。

2） 严重问题。软件问题对主要功能性能有较大影响或造成严重损失，视为严重问题：

a）没有完整实现软件需求，对主要功能性能等有较大影响；

b）没有正确实现软件需求，对主要功能性能等有较大影响；

c）造成人员、装备、环境等严重损失；

d）重要数据丢失，但能以某种方式恢复。

e） 软件文档对主要功能、性能描述缺失或错误。

3）一般问题。软件问题对软件功能性能有较小影响或造成一般损失，视为一般问题：

a）没有完整实现软件需求，对软件主要功能性能影响较小，或对一般功能性能造成影响；

b）没有正确实现软件需求，对软件主要功能性能影响较小，或对一般功能性能造成影响；

c）软件操作与软件使用说明不符；

d）重要数据丢失，但能以某种方式恢复。

e） 软件文档存在准确性、一致性、错别字等影响较小的问题。

4）建议改进：测试过程中发现的其他不方便使用或对软件功能有轻微影响的问题可提出改进建议。

### 问题处理方法

根据TE-BTCG-004-2021《军用软件鉴定测评指南》要求，问题按照如下流程进行处理。

1）测评方应按照实际情况准确记录发现的问题，填写软件问题报告单，并协同装备研制单位、任务书提出方、军事代表机构等各方共同进行问题处理；

2） 测评方应与开发方共同确认发现的软件问题

3）存在争议的问题通常应由委托方、用户、装备研制单位、软件测评机构等单位共同进行确认，必要时可邀请同行专家参加；

4） 软件问题应通过质量问题信息渠道反馈给相关装备研制单位；

5） 开发方应对每个软件问题进行定位，开展原因分析，提出修改措施，并说明修改对软件的影响。如不修改，则应说明理由及其影响和后续处理建议，并由装备研制单位或任务书提出方确认。以上内容均需在回归测评之前提交给测评方；

6） 建议改进通常也要修改。如不修改，同样应说明理由及其影响和后续处理建议，并由装备研制单位或任务书提出方确认；

7） 当问题的处理涉及到重要需求变更（例如：影响战技指标的需求，影响互联互通的需求等），或需求变更较大时，测评依据文档应联系委托方，并经过同等级的审批确认。

## 测评通过准则

软件通过鉴定测评的标准如下：

1） 软件文档齐套，内容完整，描述准确，文文一致、文实一致；

2） 软件正确实现了所规定软件功能、性能、接口、安全性等需求；

3） 软件满足规定的战术技术指标；

4） 测试中发现的软件问题（缺陷）均已进行合适处理，并通过了回归测试。

## 测评数据采信

无。

# 测评度量数据及采集要求

本次软件测评需采集的度量数据及采集要求见下表所示。

表7‑1测评度量数据及采集要求

|  |  |  |
| --- | --- | --- |
| 序号 | 需采集的度量数据 | 采集要求 |
| 1 | 软件功能点数度量 | 针对需求文档中定义的需求唯一标识进行采集 |
| 2 | 程序模块数度量 | 针对设计文档中定义的程序模块以及源程序进行采集 |
| 3 | 测试项度量 | 针对测评大纲中定义的测试项唯一标识进行采集 |
| 4 | 用例度量 | 针对测试说明中定义的测试用例唯一标识进行采集 |
| 5 | 问题度量 | 针对软件问题报告单中的问题个数进行采集，按类别和严重程度进行分类统计 |

# 测评暂停、恢复与终止

出现下列情况之一，软件测评机构应及时提出暂停鉴定测评工作的申请：

1） 测评过程中存在重大安全保密隐患；

2） 被测软件存在重大技术问题，影响测评继续开展；

3） 被测软件主要的战术技术指标达不到规定的要求；

4） 软件问题不能在规定的时限内解决或大部分问题无法达成共识。

经任务委托方批准后，鉴定测评工作可暂停，当导致暂停的问题已解决，并经软件测评总体单位（如有）、军事代表机构等相关方确认，且获得批准后可重新启动测评工作；如问题无法得到解决，获得批准后可终止鉴定测评。

# 测评组织及任务分工

测评项目组由项目负责人、项目组成员质量保证员、监督员等岗位组成，组成及职责分工见下表。

表9‑1测评项目组成员组成及职责分工

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 人员 | 岗位 | 职责 |
| 1 | 陈俊亦 | 项目负责人 | 负责组织软件测试文档的编写、设计测试用例；组织分析测试结果；编写并提交测评报告；管理测试过程。 |
| 2 | 陈俊亦、某测试人员1、某测试人员2、某测试人员3、某测试人员4 | 项目组成员 | 参与测试大纲、测试说明、测试报告的编写；参与测试执行 |
| 3 | 某质量人员 | 质量保证员 | 负责测评过程的管理 |
| 4 | 某质量人员 | 质量监督员 | 负责测评产品的监督 |
| 5 | 某质量人员 | 配置管理员 | 负责受控库被测件的接收、工作产品受控库的建立与配置管理 |

# 测评保障

## 测评条件保障

中国电子科技集团公司第三研究所负责测评设备、场地保障，主要包括测试环境提供等。

中国科学院卫星软件评测中心负责测评技术、数据保障，主要包括测试文档编写、测试用例执行等。

## 配置管理

测试过程中，项目组将严格按照评测中心配置管理的要求进行配置管理活动，保证工作产品的完整性。配置库包括开发库、受控库和产品库。

测试配置管理的对象包括测试工作产品、被测软件、测试工具及环境。

测评工作形成的工作产品包括：测评大纲、测试说明、测试记录、测评报告，及过程质量记录等，均须纳入配置管理。

由项目组配置管理员负责项目的开发库管理，中国科学院卫星软件评测中心配置管理员负责项目的受控库管理，资料管理员负责产品库管理。

软件测评设置两个基线，需求基线和产品基线，制定配置管理计划见下表所示。

表10‑1配置管理计划

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 基线  名称 | 配置管理项名称 | 标识码 | 负责人 | 基线  批准人 | 基线建立时机 | 预计基线完成时间 |
| 需求  基线 | 软件测试委托书 | / | 丁小蕊 | 施敏华 | 所有基线配置项入受控库3天内 | 2025年04月 |
| 软件需求规格说明 | / | 丁小蕊 |
| 软件设计说明 | / | 丁小蕊 |
| 使用手册 | / | 丁小蕊 |
| 产品  基线 | 测评大纲 | TO | 陈俊亦 | 施敏华 | 所有基线配置项入受控库3天内 | 2025年06月 |
| 测试说明 | TD | 陈俊亦 |
| 测试问题单 | QT | 陈俊亦 |
| 测试记录 | TN | 陈俊亦 |
| 测评报告 | TR | 陈俊亦 |
| 确定配置管理项及标识 | | | | | | |
| 配置管理项名称 | | 标识码 | 负责人 | 批准人 | 受控时机 | |
| 被测软件及文档 | | / | 陈俊亦 | 施敏华 | 被测件接收后 | |
| 测试工具及环境 | | / | 陈俊亦 | 测试环境确认后 | |
| 测评大纲 | | TO | 陈俊亦 | 评审后7个工作日内 | |
| 测试说明 | | TD | 陈俊亦 |
| 测试问题单 | | QT | 陈俊亦 |
| 测试记录 | | TN | 陈俊亦 |
| 测评报告 | | TR | 陈俊亦 |
| 配置审核时机 | | 配置项初始入库/变更入库、基线建立/变更 | | | | |

## 质量保证

### 质量保证要求

中国科学院卫星软件评测中心为该项目配备专职质量保证人员，制定项目的质量保证计划，明确需开展的评审、需保证的工作产品和项目采用的标准规范等内容。本项目需开展的评审包括测评大纲、测试说明、测评报告评审，以及测试就绪和测试总结评审等阶段管理评审。在项目开展过程中，由项目质量保证人员按照质量保证计划，对项目正在运行的过程和正在形成的工作产品开展质量保证活动，以验证它们符合相应的程序和标准。所有外发的测试工作产品都要经过质量保证人员审核。

### 质量保证计划

质量保证计划见下表所示。

表10‑2测评工作质量保证计划表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 里程碑事件 | 里程碑定义 | | 工作产品 | 计划完成时间 | |
| 需求里程碑（完成评审，可进入测试执行阶段） | | 测评大纲  测试说明 | 2025年04月 | |
| 产品里程碑（完成评审，可进入项目交付） | | 测试问题单  测评报告 | 2025年06月 | |
| 过程评审 | 评审内容 | | | 评审时间 | |
| 测试大纲评审/测试说明评审 | | | 2025年04月 | |
| 测试总结评审 | | | 2025年06月 | |
| 产品保证活动 | 工作产品 | 活动计划 | | | 工具及记录 |
| 测试大纲 | 正式评审前 | | | 工作产品审核检查单 |
| 测试说明 | 正式评审前 | | |
| 测试问题单 | 正式评审前 | | |
| 测试报告 | 正式评审前 | | |
| 过程保证活动 | 过程阶段 | 活动计划 | | | 工具及记录 |
| 测试立项 | 阶段结束 | | | 过程活动质量保证检查单 |
| 测试需求分析与策划 | 阶段结束 | | |
| 测试设计与实现 | 阶段结束 | | |
| 测试执行 | 阶段结束 | | |
| 回归测试 | 阶段结束 | | |
| 测试总结 | 阶段结束 | | |
| 归档与交付 | 阶段结束 | | |
| 质量记录 | 评审检查单、测评产品监督记录、测评过程监督记录、不符合项报告单（如果发生）、预防项报告单（如果发生） | | | | |
| 其它事项 | / | | | | |

## 评审与控制

### 设计评审

根据《军用软件鉴定测评指南》及有关规定，在软件测评过程的各阶段进行评审。通过评审（审查）后方可开展下一阶段的工作。测评工作评审项目见下表所示。

表10‑3测评工作评审项目表

| 序号 | 工作项目 | 评审形式 |
| --- | --- | --- |
| 1 | 测评大纲审查 | 外部评审 |
| 2 | 测试说明评审 | 内部评审 |
| 3 | 测试就绪评审 | 内部评审 |
| 4 | 测评总结评审 | 外部评审 |

### 过程控制

依据评测中心质量管理体系文件，对每个测试阶段及其工作项目、形式、验证文件进行规定，具体见下表。

表10‑4测评工作过程控制表

| 序号 | 工作项目 | 工作阶段 | 工作形式 | 验证文件 |
| --- | --- | --- | --- | --- |
| 1 | 测评大纲的拟制和审查 | 测试策划与测试需求分析 | 审查 | 审查意见 |
| 2 | 测试说明的拟制和评审 | 测试设计和实现 | 评审 | 评审意见 |
| 3 | 测试就绪评审 | 测试设计和实现 | 评审/检查 | 测试就绪检查表 |
| 4 | 执行测试用例，记录测试过程 | 测试执行 | 检查 | 质量检查表 |
| 5 | 编写测评报告，测评总结评审 | 测试总结 | 评审 | 评审意见 |

### 文档控制

根据测评中心质量管理体系文件，在软件测评过程的各阶段依次产生以下主要文档：测评大纲、测试说明、测试执行记录和问题报告单、测评报告。

### 人员控制

由5名符合评测中心质量管理体系中人员要求的测试人员组成测评项目组，项目负责人负责监督控制项目实施。

设置质量保证人员，负责本项目质量监督工作。

设置配置管理员，负责本项目的配置管理工作。

## 测评风险分析

测评工作可能存在如下风险，可能延缓或阻碍测试计划的如期实施，导致工作进度和测试结果受到影响。为保证测评工作顺利完成，应采取相应措施避免或消除这些风险。

测评过程的风险分析及应对措施见下表所示。

表10‑5测评风险分析

| 序号 | 风险名称 | 风险描述及风险分析 | 风险概率 | 风险后果 | 风险处理对策 |
| --- | --- | --- | --- | --- | --- |
| 1 | 人员风险 | 研制人员无法及时配合开展测试工作。 | 中 | 中 | 及时将情况上报研制总体单位和研制单位项目负责人，及时沟通、协调，安排配合测试工作。 |
| 2 | 资源风险 | 测试环境资源不能够有效的及时到位，包括实施场地、所需设备等。 | 高 | 严重 | 及时与委托方、研制单位协调相关测试环境资源。 |
| 3 | 进度风险 | 研制单位未按照规定的时间节点提供被测件，无法继续开展测试/回归测试，影响测试进度。 | 中 | 中 | 及时将情况上报，并与研制单位项目负责人，及时协调解决。 |
| 4 | 技术风险 | 研制单位提供的输入类文档不充分，缺少与软件最终状态一致的完整需求规格说明的相关功能、接口等内容，相关功能需求描述未充分体现软件具体实现逻辑设计要求。 | 中 | 大 | 加强与开发方的沟通协调。及时将情况上报总体单位，并开展文档审查，提出整改意见，催促开发人员提交完整、齐全的文档，并在测试过程中提供全面的技术支持。 |
| 5 | 信息安全保密风险 | 考虑信息安全原因，存在文件无法交付测试单位或只能由测试单位到开发单位交互信息，可能影响测试进度。 | 低 | 小 | 测试人员按计划提前规划交互内容，并保持与开发人员的沟通，提高信息交互的质量和深度。 |

## 测评分包

无。

# 测评安全与保密

为保护软件研制单位的知识产权和保守国家秘密，测评机构做出如下承诺：

1）测评项目组成员不从事与被测软件类似的软件开发工作；

2）不复制、传播和留存软件文档、程序等技术资料；

3）对软件技术资料和测评文档进行相应的保密管理；

4）未经委托方允许，不公示软件测评结果。

# 有关问题的说明

无。

# 附录A 文档审查单

## A.1 文档齐套性查单

软件文档齐套性检查单

|  |  |  |  |
| --- | --- | --- | --- |
| 项目名称 | XXX软件鉴定测评 | | |
| 项目标识 | RXXXX | | |
| 审查文档 | XXXX软件配套文档 | | |
| 审查项目 | 审查内容 | | 审查结果 |
| 齐套性 | 是否有软件任务书  是否有软件开发计划  是否有软件配置管理计划  是否有软件质量保证计划  是否有软件需求规格说明  是否有软件设计说明  是否有软件单元测试计划  是否有软件单元测试说明  是否有软件单元测试报告  是否有软件配置项测试计划  是否有软件配置项测试说明  是否有软件配置项测试报告  是否有软件用户手册  是否有软件研制总结报告  是否有软件固件保障手册  是否有软件版本说明 | | □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否  □是 □否 |
| 完整性 | 封面内容是否完整、正确，是否包括了文档名称、版本、密级、编号、单位、编写时间 | | □是 □否 |
| 文档签署是否完整，包括拟制、审核、批准等信息 | | □是 □否 |
| 规范性 | 是否有直观明了的索引（目录）和排版格式，并且正确 | | □是 □否 |
| 页眉、页脚、页码是否符合要求 | | □是 □否 |
| 审查人员 |  | 审查日期 |  |

## A.2 软件需求规格说明审查单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 文档名称 | | XXXX软件需求规格说明 | | | | |
| 版本 | | X.X.XX | | | | |
| 序号 | 审查项 | 审查内容 | 审查结果（填√） | | | 备注 |
| 通过 | 未通过 | 不适用 |
| 1 | 完整性 | 标识描述本文档所适用系统和软件的完整标识，包括其标识号、名称、缩略名、版本号和发布号 |  |  |  |  |
| 2 | 系统概述本文档适用的系统和软件的用途，描述系统与软件的一般特性 |  |  |  |  |
| 3 | 文档概述了本文档的用途和内容，并描述与它的使用有关的保密性方面的要求 |  |  |  |  |
| 4 | 引用文档应列出文档的编号、标题、编写单位、修订版及日期 |  |  |  |  |
| 5 | CSCI能力需求标识出所要求的每一个CICI能力，并列出与该能力有关的需求，包括所需的CSCI行为 |  |  |  |  |
| 6 | CSIC的外部接口需求应使用唯一的标识符标识CSCI每一个外部接口，并描述为实现该接口提出的该CSCI的需求 |  |  |  |  |
| 7 | CSCI内部接口需求应指明施加于CSCI内部接口的需求 |  |  |  |  |
| 8 | 保密性需求应指明与维护保密性有关的CSCI需求 |  |  |  |  |
| 9 | 安全性需求应指明关于防止或尽可能降低对人员、财产和物理环境产生以外危险的CSCI安全性需求 |  |  |  |  |
| 10 | 环境适应性需求应指明CSCI的运行环境需求 |  |  |  |  |
| 11 | 计算机资源需求应指明CSCI必须使用的计算机硬件的需求、计算机硬件资源的使用需求、必须使用或必须被纳入本CSCI的计算机软件需求、必须使用的计算机通信方面的需求 |  |  |  |  |
| 12 | 设计和实现约束应指明约束CSCI的设计和实现的需求 |  |  |  |  |
| 13 | 人员相关需求描述与使用或保障本CSCI的人员有关的CSCI需求，包括人员的数量、职能等级、工作周期、必须的培训以及其他信息 |  |  |  |  |
| 14 | 训练相关需求应指明与训练相关的CSCI需求 |  |  |  |  |
| 15 | 软件保障需求应指明与软件保障考虑有关的CSCI需求 |  |  |  |  |
| 16 | 包装需求应指明为了交付而对CSCI进行包装、标记和处理的需求 |  |  |  |  |
| 17 | 需求的优先顺序和关键性应指明本规格说明中各需求的优先次序、关键性或表示其相对重要性的权重 |  |  |  |  |
| 18 | 合格性规定应定义一组合格性检验方法，针对每个需求制定确定需求得到满足所使用的方法 |  |  |  |  |
| 19 | 需求可追踪性应描述从本规格说明中的每一个CSCI需求所涉及的系统/子系统需求的可追踪性，以及从分配给本CSCI的每一个系统/子系统需求，到所涉及的CSCI需求的可追踪性 |  |  |  |  |
| 20 | 准确性 | 对各项需求项目的描述准确无歧义 |  |  |  |  |
| 21 | 列举的各项需求均具备可测试性 |  |  |  |  |
| 22 | 在已知的条件限制下，所有的需求都应为可实现的需求 |  |  |  |  |
| 23 | 一致性 | 各项需求之间无相互矛盾或冲突 |  |  |  |  |
| 24 | 需求规格说明与其他软件文档之间无相互矛盾或冲突 |  |  |  |  |

## A.3 软件设计文档审查单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 文档名称 | | XXXX软件设计说明 | | | | |
| 版本 | | X.X.XX | | | | |
| 序号 | 审查项 | 审查内容 | 审查结果（填√） | | | 备注 |
| 通过 | 未通过 | 不适用 |
| 1 | 完整性 | 标识描述本文档所适用系统和软件的完整标识，包括其标识号、名称、缩略名、版本号和发布号 |  |  |  |  |
| 2 | 系统概述本文档适用的系统和软件的用途，描述系统与软件的一般特性 |  |  |  |  |
| 3 | 文档概述了本文档的用途和内容，并描述与它的使用有关的保密性方面的要求 |  |  |  |  |
| 4 | 引用文档应列出文档的编号、标题、编写单位、修订版及日期 |  |  |  |  |
| 5 | CSCI级设计决策应根据需要分条给出CSCI行为设计的决策和其他影响组成该CSCI的软件单元的选择与设计的决策 |  |  |  |  |
| 6 | CSCI部件描述构成该CSCI的所有软件单元、软件单元的静态关系、每个软件单元的用途、每个软件单元的开发状态/类型、CSCI计划使用的计算机硬件资源、标识实现每个软件单元的软件放置在哪个程序库中 |  |  |  |  |
| 7 | 执行方案应说明软件单元间的执行方案，说明软件单元间的动态关系 |  |  |  |  |
| 8 | 接口标识和接口图应标识每一个接口，包含项目唯一的标识符，并声明哪些实体具有固定的接口特性，说明哪些实体正在开发或修改之中 |  |  |  |  |
| 9 | 通过唯一的标识符来标识接口，并标识接口实体，分条描述单方或双方接口实体的特性 |  |  |  |  |
| 10 | CSCI详细设计应通过项目唯一的标识符来标识软件单元，并对该单元进行说明  a）单元设计决策  b）该软件单元设计中的任何约束、限定或非常规特征  c）如果使用的编程语言不同于该CSCI所指定的语言，则应指出并说明使用它的理由  d）如果该软件单元包含过程性命令或由过程性命令组成，应列出这些过程性命令，并引用解释它们的用户手册或其他文档  e）如果该软件单元包含、接收或输出数据，应对它的输入、输出及其他数据元素和数据元素组合体进行说明  f）如果该软件单元包含逻辑，则给出该软件单元所用到的逻辑 |  |  |  |  |
| 11 | 需求可追踪性包含从本文档所标识的每个软件单元，到分配给它的CSCI需求的可追踪性，以及从每个CSCI需求，到被分配这些需求的软件单元的可追踪性。 |  |  |  |  |
| 12 | 准确性 | 程序流程图、时序图等符合标准规范 |  |  |  |  |
| 13 | 所有的变量说明和模块说明均清晰无歧义 |  |  |  |  |
| 14 | 所有的文字和图形应描述清晰准确 |  |  |  |  |
| 15 | 无二义性的定义、术语或内容 |  |  |  |  |
| 16 | 一致性 | 设计文档上下文一致无冲突 |  |  |  |  |
| 17 | 设计文档中图文一致无冲突 |  |  |  |  |
| 18 | 设计文档与需求文档一致，无冲突 |  |  |  |  |

# 附录B 代码审查单

## B.1 C语言代码审查单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 审查内容 | | 审查结果（填√） | | | 备注 |
| 通过 | 未通过 | 不适用 |
|  | 存储类 | 未使用内存的内容是否影响系统安全  其处理是否得当 |  |  |  |  |
|  | 动态申请内存是否判断成功后使用 |  |  |  |  |
|  | 动态分配的内存是否及时释放 |  |  |  |  |
|  | 防止内存操作越界 |  |  |  |  |
|  | 声明定义 | 变量是否正确定义 |  |  |  |  |
|  | 不同标识符的书写是否清晰可辨 |  |  |  |  |
|  | 数组声明时，其大小是否定义好 |  |  |  |  |
|  | 共用体、结构体、枚举的所有成员变量是否进行了初始化 |  |  |  |  |
|  | 指针使用 | 是否存在指针越界（指针指向的地址不超过了有效地址范围） |  |  |  |  |
|  | 不应将局部变量的地址赋值给外部指针 |  |  |  |  |
|  | 是否对参数指针进行赋值 |  |  |  |  |
|  | 参数变量的传递是否使用了无类型指针 |  |  |  |  |
|  | 是否使用了野指针 |  |  |  |  |
|  | 类型转换 | 数据类型转换是否正确 |  |  |  |  |
|  | 隐式的整型转换是否改变了基础类型的符号 |  |  |  |  |
|  | 整型或浮点的隐式转换是否缩小了基础类型的大小 |  |  |  |  |
|  | 指针变量赋予非指针变量时是否进行了强制转换 |  |  |  |  |
|  | 是否使用无实质作用的类型转换 |  |  |  |  |
|  | 比较判断 | 是否进行了浮点相等比较（不能进行浮点相等比较，也不能与0值进行相等比较，包括不等于的比较，只能进行大于小于的比较） |  |  |  |  |
|  | 是否对无符号数进行大于或等于零或小于零的比较 |  |  |  |  |
|  | 变量有效性判断时范围是否与文档一致 |  |  |  |  |
|  | 是否使用指针进行大于或小于的逻辑比较 |  |  |  |  |
|  | 数学运算 | 选择的运算符合理吗？运算符的优先结合次序正确吗？ |  |  |  |  |
|  | 应对运算中可能存在的数据溢出（如除数为零、大数相加减乘除、数据连续加、数据连续减、根号下为负数等）情况进行处理 |  |  |  |  |
|  | 是否将bool类型用做内置运算符的操作数？（除了&&、||、!、==、!=、&和条件运算符） |  |  |  |  |
|  | 是否将enum类型用作内置运算符的操作数？（除了[]、=、==、!=、&、<、<-、>、->运算符） |  |  |  |  |
|  | 运算符!、&&或||的每个操作数是否都是bool类型？ |  |  |  |  |
|  | 对变量进行移位运算是否超出变量长度 |  |  |  |  |
|  | 是否将越界整数赋给整型变量 |  |  |  |  |
|  | 数组下标是否是大于等于零的整型数 |  |  |  |  |
|  | 非枚举类型变量是否使用了枚举类型的值 |  |  |  |  |
|  | 是否存在一个很大的数与一个很小的数进行+，-运算 |  |  |  |  |
|  | 是否给无符号类型变量赋负值 |  |  |  |  |
|  | 数据精度是否满足运算要求 |  |  |  |  |
|  | 需要时，应对运算进行正确的限幅（输出的结果是否有上下限要求） |  |  |  |  |
|  | 变量的定义类型和使用类型是否一致 |  |  |  |  |
|  | 函数使用 | 函数是否返回了定义在函数内部的局部变量 |  |  |  |  |
|  | 有返回值函数的返回语句是否带有返回值 |  |  |  |  |
|  | 全部所需的参数是否已传送给每一个被调用的模块（参数传的全不全） |  |  |  |  |
|  | 被传送的参数值是否正确的设置 |  |  |  |  |
|  | 函数定义与声明一致 |  |  |  |  |
|  | 函数的错误返回值都必须进行处理 |  |  |  |  |
|  | 实参和形参所使用的变量类型和个数是否一致 |  |  |  |  |
|  | 程序语言的使用 | 文件、数据库和注册表等打开后，在对其进行操作之后是否进行了关闭 |  |  |  |  |
|  | 用于表示字符串的数组是否以‘\0’结束 |  |  |  |  |
|  | 函数宏参数的定义是否使用括号 |  |  |  |  |
|  | for循环中控制变量是否为局部变量 |  |  |  |  |
|  | for循环中控制变量是否为整型变量 |  |  |  |  |
|  | for循环中是否对循环控制变量进行修改 |  |  |  |  |
|  | 寄存器使用 | 寄存器使用是否按照芯片手册的操作要求 |  |  |  |  |
|  | 宏扩展或子程序调用是否使用了已使用着的寄存器而未保存数据 |  |  |  |  |
|  | 默认使用的寄存器的值是否正确（注意每个寄存器的初始默认值） |  |  |  |  |
|  | 可维护性 | 嵌套的IF、ELSE、WHILE等语句是否已正确地缩进、是否少括号，是否忘写了括号 |  |  |  |  |
|  | 注释准确并且有意义 |  |  |  |  |
|  | 注释语句应不少于20 |  |  |  |  |
|  | 是否存在嵌套注释 |  |  |  |  |
|  | 标号和子程序名符合代码的逻辑含义吗 |  |  |  |  |
|  | 避免使用不易理解的数字，用有意义的标识来替代，涉及物理状态或者含有物理意义的常量，不应直接使用数字，必须用有意义的枚举或宏来代替 |  |  |  |  |
|  | 注意运算符的优先级，并用括号明确表达式的操作顺序，避免使用默认优先级 |  |  |  |  |
|  | 逻辑 | 代码是否做了设计规定的内容 |  |  |  |  |
|  | 全部设计是否均已实现（和详细设计的一致性） |  |  |  |  |
|  | 每个循环是否执行正确的次数 |  |  |  |  |
|  | 是否存在死循环的风险（例如当等待某变量为一特定值才退出时存在风险；循环语句中必须有超时保护） |  |  |  |  |
|  | 不能使用未赋值的变量 |  |  |  |  |
|  | Switch语句必须有default分支 |  |  |  |  |
|  | 必须处理程序所能遇到的各种出错情况 |  |  |  |  |
|  | 软件多余物 | 是否有不可能执行到的代码 |  |  |  |  |
| 是否有即使不执行也不影响程序功能的指令 |  |  |  |  |
| 是否有未引用的变量、标号和常量 |  |  |  |  |
|  | 有无未引用的宏 |  |  |  |  |
|  | 其他 | 应根据看门狗触发周期正确设置其清除周期（不能超过狗咬时间） |  |  |  |  |
|  | 应根据需要监视的流程，正确设置清除看门狗的位置（在该清除的地方要清除，比如初始化阶段、各个进程等；在不该清除的地方不能清除，比如在需求中要求等待狗咬的位置等） |  |  |  |  |
|  | 对于全局变量的读写要合理 |  |  |  |  |
|  | 代码审查覆盖项 | 中断资源冲突检查 |  |  |  |  |

# 附录C 静态分析审查单

## C.1 代码质量度量分析表单

质量度量要求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 软件名称 | | XXX软件 | | | |
| 软件版本 | | X.X.XX | | 软件规模 | XXXX |
| 代码行 | | XXXX | | 注释行 | XXXX |
| 模块总数（个） | |  | | 空行 | XXXX |
| 度量元 | 描述 | | 判别标准 | 实测结果 | 是否满足 |
| 平均规模 | 模块规模之和/模块数 | | ≤200行 |  |  |
| 平均扇出数 | 模块扇出数之和/模块数 | | ≤7 |  |  |
| 平均圈复杂度 | 模块圈复杂度之和/模块数 | | ≤10 |  |  |
| 模块最大圈复杂度 | 各模块圈复杂度的最大值 | | ≤80 |  |  |
| 圈复杂≥20 的比例 | 模块中圈复杂度≥20 的个数占总模块数的个数和百分比； | | ≤20% |  |  |
| 注释率 | 注释行数/代码行数\*100% | | ≥20% |  |  |

## C.2 代码编码规则表

编码规则要求

|  |  |  |
| --- | --- | --- |
| 规则编号 | 规则描述 | 违反规则代码 |
| R-1-1-1 | 禁止通过宏定义改变关键字和基本类型含义 |  |
| R-1-1-2 | 禁止将其他标识宏定义为关键字和基本类型 |  |
| R-1-1-3 | 用typedef自定义的类型禁止被重新定义 |  |
| R-1-1-4 | 禁止重新定义C或C++的关键字 |  |
| R-1-1-5 | 禁止#define被重复定义 |  |
| R-1-1-6 | 函数中的#define和#undef必须配对使用 |  |
| R-1-1-7 | 以函数形式定义的宏，参数和结果必须用括号括起来 |  |
| R-1-1-8 | 结构、联合、枚举的定义中必须定义标识名 |  |
| R-1-1-9 | 结构体定义中禁止含有无名结构体 |  |
| R-1-1-10 | 位定义的有符号整型变量位长必须大于1 |  |
| R-1-1-11 | 位定义的整数型变量必须明确定义是有符号还是无符号的 |  |
| R-1-1-12 | 位定义的变量必须是同长度的类型且定义位禁止跨越类型的长度 |  |
| R-1-1-13 | 函数声明中必须对参数类型进行声明，并带有变量名 |  |
| R-1-1-14 | 函数声明必须与函数原型一致 |  |
| R-1-1-15 | 函数中的参数必须使用类型声明 |  |
| R-1-1-16 | 外部声明的变量，类型必须与定义一致 |  |
| R-1-1-17 | 禁止在函数体内使用外部声明 |  |
| R-1-1-18 | 数组定义禁止没有显示的边界限定 |  |
| R-1-1-19 | 禁止使用extern声明对变量初始化 |  |
| R-1-1-20 | 用于数值计算的字符型变量必须明确定义是有符号还是无符号 |  |
| R-1-1-21 | 禁止在#include语句中使用绝对路径 |  |
| R-1-1-22 | 禁止头文件重复包含 |  |
| R-1-1-23 | 函数参数表为空时，必须使用void明确说明 |  |
| R-1-2-1 | 循环体必须用大括号括起来 |  |
| R-1-2-2 | If、else if、else必须用大括号括起来 |  |
| R-1-2-3 | 禁止在头文件前有可执行代码 |  |
| R-1-2-4 | 引起二义性理解的逻辑表达式，必须使用括号显式说明优先级顺序 |  |
| R-1-2-5 | 逻辑判别表达式中的运算项必须要使用括号 |  |
| R-1-2-6 | 禁止嵌套注释 |  |
| R-1-3-1 | 禁止指针的指针超过两级 |  |
| R-1-3-2 | 函数指针的使用必须加以&明确说明 |  |
| R-1-3-3 | 禁止对参数指针进行赋值 |  |
| R-1-3-4 | 禁止将局部变量地址做为函数返回值返回 |  |
| R-1-3-5 | 禁止使用或释放未分配空间或已释放的指针 |  |
| R-1-3-6 | 指针变量被释放后必须置为NULL |  |
| R-1-3-7 | 动态分配的指针变量定义时如未被分配空间必须初始化为NULL |  |
| R-1-3-8 | 动态分配的指针变量第一次使用前必须进行是否为NULL的判别 |  |
| R-1-3-9 | 空指针必须使用NULL，禁止使用整型数0 |  |
| R-1-3-10 | 禁止文件指针在退出时没有关闭文件 |  |
| R-1-4-1 | 在if-else if语句中必须使用else分支 |  |
| R-1-4-2 | 条件判定分支如果为空，必须以单独一行的分号加注释进行明确说明 |  |
| R-1-4-3 | 禁止使用空switch语句 |  |
| R-1-4-4 | 禁止对bool量使用switch语句 |  |
| R-1-4-5 | 禁止switch语句中只包含default语句 |  |
| R-1-4-6 | 除枚举类型列举完全外，switch语句必须要有default |  |
| R-1-4-7 | Switch中的case和default必须以break或return终止，共用case必须加以明确注释 |  |
| R-1-4-8 | Switch语句的所有分支必须具有相同的层次范围 |  |
| R-1-5-1 | 禁止从复合语句外goto到复合语句内，或由下向上goto |  |
| R-1-5-2 | 禁止使用setjmp/longjmp |  |
| R-1-6-1 | 禁止将浮点常数赋值给整型变量 |  |
| R-1-6-2 | 禁止将越界整数赋值给整型变量 |  |
| R-1-6-3 | 禁止在逻辑表达式中使用赋值语句 |  |
| R-1-6-4 | 禁止对逻辑表达式进行位运算 |  |
| R-1-6-5 | 禁止在运算表达式中或函数调用参数中使用++或—操作符 |  |
| R-1-6-6 | 对变量进行移位运算禁止超出变量长度 |  |
| R-1-6-7 | 禁止移位操作中的移位数为负数 |  |
| R-1-6-8 | 数组禁止越界使用 |  |
| R-1-6-9 | 数组下标必须是大于等于零的整型数 |  |
| R-1-6-10 | 禁止对常数值做逻辑非的运算 |  |
| R-1-6-11 | 禁止非枚举类型变量使用枚举类型的值 |  |
| R-1-6-12 | 除法运算中禁止被零除 |  |
| R-1-6-13 | 禁止在sizeof中使用赋值 |  |
| R-1-6-14 | 缓存区读取操作禁止越界 |  |
| R-1-6-15 | 缓存区写入操作禁止越界 |  |
| R-1-6-16 | 禁止使用已被释放了的内存空间 |  |
| R-1-6-17 | 被free的指针必须指向最初malloc、calloc分配的地址 |  |
| R-1-6-18 | 禁止使用gets函数，应使用fgets函数替代 |  |
| R-1-6-19 | 使用字符串赋值、拷贝、追加等函数时，禁止目标字符串存储空间越界 |  |
| R-1-7-1 | 禁止覆盖标准函数库的函数 |  |
| R-1-7-2 | 禁止函数的实参和形参类型不一致 |  |
| R-1-7-3 | 实参和形参的个数必须一致 |  |
| R-1-7-4 | 禁止使用旧形式的函数参数表定义形式 |  |
| R-1-7-5 | 函数声明和函数定义中的参数类型必须一致 |  |
| R-1-7-6 | 函数声明和函数定义中的返回类型必须一致 |  |
| R-1-7-7 | 有返回值的函数必须通过返回语句返回 |  |
| R-1-7-8 | 禁止无返回值函数的返回语句带有返回值 |  |
| R-1-7-9 | 有返回值的函数的返回语句必须带有返回值 |  |
| R-1-7-10 | 函数返回值的类型必须与定义一致 |  |
| R-1-7-11 | 具有返回值的函数，其返回值如果不被使用，调用时应有（void）说明 |  |
| R-1-7-12 | 无返回值的函数，调用时禁止再用（void）重复说明 |  |
| R-1-7-13 | 静态函数必须被使用 |  |
| R-1-7-14 | 禁止同一个表达式中调用多个顺序相关函数 |  |
| R-1-7-15 | 禁止在函数参数表中使用省略号 |  |
| R-1-7-16 | 禁止使用直接或间接自调用函数 |  |
| R-1-8-1 | 禁止不可达语句 |  |
| R-1-8-2 | 禁止不可达分支 |  |
| R-1-8-3 | 禁止使用无效语句 |  |
| R-1-8-4 | 使用八进制数必须明确注释 |  |
| R-1-8-5 | 数字类型后缀必须使用大写字母 |  |
| R-1-9-1 | For循环控制变量必须使用局部变量 |  |
| R-1-9-2 | For循环控制变量必须使用整数型变量 |  |
| R-1-9-3 | 禁止在for循环体内部修改循环控制变量 |  |
| R-1-9-4 | 无限循环必须使用while(1)语句，禁止使用for(;;)等其他形式的语句 |  |
| R-1-10-1 | 浮点数变量赋值给整型变量必须强制转换 |  |
| R-1-10-2 | 长整数变量赋值给短整数变量必须强制转换 |  |
| R-1-10-3 | Double型变量赋给float型变量必须强制转换 |  |
| R-1-10-4 | 指针变量的赋值类型必须与指针变量类型一致 |  |
| R-1-10-5 | 将指针量赋予非指针变量或非指针量赋予指针变量，必须使用强制转换 |  |
| R-1-10-6 | 禁止使用无实质作用的类型转换 |  |
| R-1-11-1 | 变量禁止未赋值就使用 |  |
| R-1-11-2 | 变量初始化禁止隐含依赖于系统的缺省值 |  |
| R-1-11-3 | 结构体初始化的嵌套结构必须与定义一致 |  |
| R-1-11-4 | 枚举元素定义中的初始化必须完整 |  |
| R-1-12-1 | 禁止对逻辑量进行大于或小于的逻辑比较 |  |
| R-1-12-2 | 禁止对指针进行大于或小于的逻辑比较 |  |
| R-1-12-3 | 禁止对浮点数进行是否相等的比较 |  |
| R-1-12-4 | 禁止对无符号数进行大于等于零或小于零的比较 |  |
| R-1-12-5 | 禁止无符号数与有符号数之间的直接比较 |  |
| R-1-13-1 | 禁止局部变量与全局变量同名 |  |
| R-1-13-2 | 禁止函数形参与全局变量同名 |  |
| R-1-13-3 | 禁止变量名与函数名同名 |  |
| R-1-13-4 | 禁止变量名与标识名同名 |  |
| R-1-13-5 | 禁止变量名与枚举元素同名 |  |
| R-1-13-6 | 禁止变量名与typedef自定义的类型名同名 |  |
| R-1-13-7 | 禁止在内部块中重定义已有的变量名 |  |
| R-1-13-8 | 禁止仅依赖大小写区分的变量 |  |
| R-1-13-9 | 禁止仅依赖小写字母“l”与数字“1”区分的变量 |  |
| R-1-13-10 | 禁止仅依赖小写字母“O”与数字“0”区分的变量 |  |
| R-1-13-11 | 禁止单独使用小写字母“l”或大写字母“O”作为变量名 |  |
| R-1-13-12 | 程序外部可改写的变量，必须使用volatile类型说明 |  |
| R-1-13-13 | 禁止在表达式中出现多个同一volatile类型变量的运算 |  |
| R-1-13-14 | 禁止将NULL做为整型数0使用 |  |
| R-1-13-15 | 禁止给无符号类型变量赋负值 |  |
| R-1-13-16 | 用于表示字符串的数组必须以‘\0’结束 |  |
| R-2-1-1 | 含有动态分配成员的类，必须编写拷贝构造函数，并重载赋值操作符 |  |
| R-2-1-2 | 虚拟基类指针转换为派生类指针必须使用dynamic cast转换 |  |
| R-2-1-3 | 菱形层次结构的派生设计，对基类派生必须使用virtual说明 |  |
| R-2-1-4 | 抽象类中的复制操作符重载必须是保护的或私有的 |  |
| R-2-2-1 | 构造函数中禁止使用全局变量 |  |
| R-2-2-2 | 类中必须明确定义缺省构造函数 |  |
| R-2-2-3 | 单参数构造函数必须使用explicit声明 |  |
| R-2-2-4 | 类中所有成员变量必须在构造函数中初始化 |  |
| R-2-2-5 | 派生类构造函数必须在初始化列表中说明直接基类构造函数 |  |
| R-2-3-1 | 具有虚拟成员函数的类，析构函数必须是虚拟的 |  |
| R-2-3-2 | 析构函数中禁止存在不是由自身捕获处理的异常 |  |
| R-2-4-1 | 基类虚拟函数的参数缺省值在派生类重写函数中禁止被改变 |  |
| R-2-4-2 | 派生类对基类虚拟函数重写的声明必须使用virtual显示说明 |  |
| R-2-4-3 | 禁止非纯虚函数被纯虚函数重写 |  |
| R-2-5-1 | 禁止将不相关的指针类型强制转换为对象指针类型 |  |
| R-2-5-2 | 指针或引用的类型转换中禁止移除const或volatile属性 |  |
| R-2-6-1 | 使用new分配的内存空间，用完后必须使用delete释放 |  |
| R-2-6-2 | 必须使用delete[]释放new[]分配的内存空间 |  |
| R-2-6-3 | 被delete的指针必须指向最初new分配的地址 |  |
| R-2-7-1 | 函数中固定长度数组变量的传递必须使用引用方式 |  |
| R-2-7-2 | 定义为const的成员函数禁止返回非const的指针或引用 |  |
| R-2-7-3 | 禁止可导致非资源性对象数据被外部修改的成员函数返回 |  |
| R-2-8-1 | 捕获的顺序必须按由派生类到基类的次序排序 |  |
| R-2-8-2 | 每个指定的抛出必须由与之匹配的捕获 |  |
| R-2-8-3 | 异常抛出的对象必须使用引用方式捕获 |  |
| R-2-8-4 | 缺省捕获必须放在所有指定捕获之后 |  |
| R-2-8-5 | 禁止显式直接抛出NULL |  |
| R-2-9-1 | 模板的声明、定义与实现必须在同一个文件之中 |  |

## C.3 控制流分析表单

控制流分析要求及结果说明表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 控制流分析记录单 | | | | |
| 序号 | 控制流分析要求 | | | |
| 1. | 是否存在转向并不存在的语句标号？（错误） | | | |
| 2. | 是否存在调用不存在的子程序？（错误） | | | |
| 3. | 是否存在不合理的无限循环结构？（提示：无限循环多与中断函数配合使用，应分析其是否符合设计要求）（错误） | | | |
| 4. | Switch语句的索引变量的数值是否与可能的分支数量不同？（错误） | | | |
| 5. | 是否存在不能穷尽的判断？（如：一个输入参数的预期是1、2或3，当参数值部位1和2时，是否在逻辑上假设了参数值必定为3）（错误） | | | |
| 6. | 是否存在go to语句的程序转向结构？（警告） | | | |
| 7. | 是否存在未使用的子程序定义或语句标号？（提示：测试工具分析的未调用模块多为中断程序模块，应分析实际运行过程中模块能够被调用）（警告） | | | |
| 8. | 是否存在函数的递归调用？（警告） | | | |
| 9. | 是否存在多个函数出口？（警告） | | | |
| 10. | 是否存在从程序入口进入后无法达到的语句或分支（不可达语句）?（提示：测试工具分析的不可达语句或分支多为异常或可靠性处理，应确认其是否符合设计）（警告） | | | |
| 11. | 循环体中存在循环中断（break）或强制循环（continue）的非结构化设计时，是否符合设计要求？（警告） | | | |
| 分析结果说明 | | | | |
| 问题 | | | 位置 | 问题报告单编号 |
| （说明问题违反了哪项控制流分析要求，如问题不包括在上述列出的内容，可写为“其他问题”，如果未发现问题则直接填写“——”） | | | （说明问题所在位置，如果某个程序文件的第几行，或某个函数单元的第几行） | （说明描述软件问题的问题单编号） |
| … | | | … | … |
| 控制流分析结论 | | 根据分析结果，给出分析结论。  （示例：对软件进行控制流分析，存在如下违反控制流分析检查要求的情况：  第1项：是否存在转向并不存在的语句标号；  …。  或对软件进行控制流分析，无违反控制流分析检查要求的情况。） | | |

## C.4 数据流分析表单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据流分析记录单 | | | | |
| 序号 | 数据流分析要求 | | | |
| 1. | 是否存在变量（对象）使用前未定义的情况（-u）？（错误） | | | |
| 2. | 是否存在变量（对象）未定义或销毁之后再使用（ku）？（错误） | | | |
| 3. | 是否存在变量（对象）在两次定义间未被使用的情况（dd）？（警告） | | | |
| 4. | 是否存在变量（对象）定义但未被使用的情况（d-）？（警告） | | | |
| 5. | 是否存在变量（对象）未定义或销毁之后再销毁（kk）？（警告） | | | |
| 6. | 是否存在变量（对象）定义之后销毁（dk）？（警告） | | | |
| 7. | 是否存在变量（对象）定义之前销毁（-k）？（警告） | | | |
| 分析结果说明 | | | | |
| 问题 | | | 位置 | 问题报告单编号 |
| （说明问题违反了哪项数据流分析要求，如问题不包括在上述列出的内容，可写为“其他问题”，如果未发现问题则直接填写“——”） | | | （说明问题所在位置，如果某个程序文件的第几行，或某个函数单元的第几行） | （说明描述软件问题的问题单编号） |
| … | | | … | … |
| 数据流分析结论 | | 根据分析结果，给出分析结论。  （示例：对软件进行数据流分析，存在如下违反数据流分析检查要求的情况：  第1项：是否存在变量（对象）使用前未定义的情况；  …。  或对软件进行数据流分析，无违反数据流分析检查要求的情况。） | | |

# 附录D 软件需求与测试需求对照表

## D.1 测试需求与研制总要求（或技术协议）覆盖情况表

测试项与研制总要求对照表

| 研制总要求 | | | 测评大纲 | | |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节号 | 描述 | 大纲章节号 | 测试项 | 标识 |

## D.2 测试需求与需求规格说明覆盖情况表

需求规格说明与测试项对照表

| 系统规格说明 | | | 测评大纲 | | |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节号 | 描述 | 大纲章节号 | 测试项 | 标识 |
|  | / | / | 6.2.2.1 | 静态分析 | XQ\_SA\_JTFX |
|  | / | / | 6.2.3.1 | 代码审查 | XQ\_CR\_DMSC |
|  | / | / | 6.2.1.1 | 文档审查 | XQ\_DC\_WDSC |
|  | 3.2.2.1.1 | 探测显示功能 | 6.2.4.1 | 探测显示功能测试 | XQ\_SU\_TCXS |
|  | / | 切换相对时统误差 | 6.2.6.1 | 切换相对时统误差摸底测试 | XQ\_MD\_XDST |
|  | 3.2.2.2.6 | 数据记录功能模块 | 6.2.4.2 | 数据储存时间性能 | XQ\_SU\_CCSJ |
|  | 3.3 | 与声探测信号处理软件接口 | 6.2.5.1 | 与声探测信号处理软件接口 | XQ\_IO\_INT1 |

测试项与需求规格说明对照表

| 测评大纲 | | | | 需求规格说明 | |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节号 | 测试项 | 标识 | 大纲章节号 | 描述 |
|  | 6.2.2.1 | 静态分析 | XQ\_SA\_JTFX | / | / |
|  | 6.2.3.1 | 代码审查 | XQ\_CR\_DMSC | / | / |
|  | 6.2.1.1 | 文档审查 | XQ\_DC\_WDSC | / | / |
|  | 6.2.4.1 | 探测显示功能测试 | XQ\_SU\_TCXS | 3.2.2.1.1 | 探测显示功能 |
|  | 6.2.6.1 | 切换相对时统误差摸底测试 | XQ\_MD\_XDST | / | 切换相对时统误差 |
|  | 6.2.4.2 | 数据储存时间性能 | XQ\_SU\_CCSJ | 3.2.2.2.6 | 数据记录功能模块 |
|  | 6.2.5.1 | 与声探测信号处理软件接口 | XQ\_IO\_INT1 | 3.3 | 与声探测信号处理软件接口 |