|  |  |
| --- | --- |
| 标识：PT-RXXXX-TN | 鉴定文件 |

XXXX

XXXX软件

鉴定测试记录

册号：1/1 总页数：55

**中国科学院卫星软件评测中心**

XX年XX月XX日

XXXX软件

鉴定测试记录

**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**

目 录

[1 范围 2](#_Toc196383576)

[1.1 标识 2](#_Toc196383577)

[1.2 被测软件信息 3](#_Toc196383578)

[2 测试记录 3](#_Toc196383579)

[2.1 文档审查测试 3](#_Toc196383580)

[附录A 文档审查单 5](#_Toc196383581)

[A.1 文档齐套性查单 5](#_Toc196383582)

[A.2 软件需求规格说明审查单 5](#_Toc196383583)

[A.3 软件设计文档审查单 7](#_Toc196383584)

[附录B 代码审查单 9](#_Toc196383585)

[B.1 C语言代码审查单 9](#_Toc196383586)

[附录C 静态分析审查单 13](#_Toc196383587)

[C.1 代码质量度量分析表单 13](#_Toc196383588)

[C.2 代码编码规则表 14](#_Toc196383589)

[C.3 控制流分析表单 21](#_Toc196383590)

[C.4 数据流分析表单 22](#_Toc196383591)

XXXX软件鉴定测评大纲

# 范围

## 标识

1）文档标识号：PT-RXXXX-TN

2）本文档的标题：XXXX软件鉴定测试记录

3）本文档适用的范围：定义“XXXX软件”的测试记录

## 被测软件信息

本次测评对象基本信息见下表。

表1‑1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 | XXX软件 | 新研 | C | XXXX | XXXX | C  C++ | XXXX | XXX | XX-XX-XX | XXXXX |

# 测试记录

## 文档审查测试

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
| 测试用例名称 | | 文档审查 | | | 标 识 | | YL\_DC | |
| 追踪关系 | | 软件测试依据：测试需求规格说明  测试需求分析：（3.4.1）文档审查  测试需求标识：XQ\_DC | | | | | | |
| 测试用例综述 | | 按测试需求中附录A中文档齐套性检查单检查需求类、设计类、用户类、测试类文档是否齐套 | | | | | | |
| 用例初始化 | | 文档已提交 | | | | | | |
| 前提和约束 | | 提交的文档出自委托方受控库，是委托方正式签署外发的 | | | | | | |
| 测试步骤 | | | | | | | | |
| 序号 | 输入及操作 | | 期望结果与评估标准 | | | 实测结果 | | 通过  与否 |
| 1 |  | |  | | |  | |  |
| 执行状态 | |  | | 测试时间 | |  | | |
| 测试人员 | |  | | 监测人员 | |  | | |
| 问题单标识 | |  | | | | | | |
| 备注 | |  | | | | | | |

# 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 | XXXX软件鉴定测评 | | |
| 项目标识 | XXXX | | |
| 审查文档 | 声探测信息交互无敌软件配套文档 | | |
| 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 | XXXX | 审查日期 | XX年XX月XX日 |

## 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 | | XXXX | | | | |
| 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 | | XXXX | | | | |
| 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 | | XXXX软件 | | | |
| 软件版本 | | 4.A.00 | | 软件规模 | 24791 |
| 代码行 | | 22703 | | 注释行 | 13624 |
| 模块总数（个） | |  | | 空行 | 1200 |
| 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。） | | |