

T/HBSGX

湖北省光电显示行业协会团体标准

T/HBSGX 003—2025

显示终端嵌入式软件设计与验证规范

Display terminal embedded software design and verification specification

2025 - 12 - 01 发布

2025 - 12 - 01 实施

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。

本文件由四川信融慧创科技有限公司提出。

本文件由湖北省光电显示行业协会归口。

本文件起草单位：四川信融慧创科技有限公司、成都瑞天芯诚信息技术服务有限公司、成都中发华茂科技有限公司、成都航幡芯海科技有限公司、成都大力优划科技有限公司。

本文件主要起草人：罗圆圆、刘涛、方苗、文东川、朱明三。

全国团体标准

显示终端嵌入式软件设计与验证规范

1 范围

本文件规定了显示终端嵌入式软件的设计原则、总体要求、设计要求、验证要求以及文档管理要求。本文件适用于显示终端嵌入式软件设计、实施及验证。

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 8566-2022 系统与软件工程 软件生存周期过程

GB/T 11457-2006 信息技术 软件工程术语

GB/T 22033-2017 信息技术 嵌入式系统术语

GB/T 28169 嵌入式软件 C语言编码规范

GB/T 30961 嵌入式软件质量度量

3 术语和定义

GB/T 11457-2006、GB/T 22033-2017界定的以及下列术语和定义适用于本文件。

3.1

模块化设计 modular design

将软件系统按功能划分为若干个独立可复用的模块，模块内部高内聚（功能关联性强）、模块间低耦合（接口依赖弱），通过标准化接口实现交互的设计方法。

3.2

嵌入式软件 embedded software

由制造商提供的软件，是产品的组成部分，可以进行部分修改。

[来源：GB/Z 41912-2022，3.1]

3.3

实时性 real-time

软件在规定的窗口内完成任务或响应外部事件的能力，通常以任务执行周期、响应延迟为量化指标。

4 设计原则与总体要求

4.1 设计原则

4.1.1 模块化原则

4.1.1.1 嵌入式软件应采用模块化设计，每个模块应具备单一明确、完整的功能。

4.1.1.2 模块间应通过标准化接口交互，接口应包含输入参数、输出参数、数据类型、错误码及调用约束。

4.1.1.3 单个模块的非空代码行数不宜超过 5000 行，超过时宜进一步拆分。

4.1.2 可移植性原则

4.1.2.1 图像缩放、色彩校正等核心算法应与硬件驱动分离，避免直接操作硬件寄存器。

4.1.2.2 支持至少 2 种主流嵌入式处理器架构，架构适配通过条件编译实现，不修改核心逻辑代码。

4.1.3 安全性原则

4.1.3.1 如固件更新、工厂校准参数修改等敏感操作应实施权限分级控制，至少包含“用户级”（仅可读取）和“管理员级”（可修改）两级权限。

4.1.3.2 嵌入式软件的关键配置数据应采用加密存储，防止未授权篡改。

4.1.4 可靠性原则

4.1.4.1 嵌入式软件应具备故障检测与恢复机制，如检测到显示驱动超时，应自动重启驱动模块并记录故障日志。

4.1.4.2 应对外部输入数据（如用户设置的亮度值）进行有效性校验，拒绝超出合理范围的输入。

4.1.5 软件质量度量

嵌入式软件应依据GB/T 30961对内部质量模型、外部质量模型和使用质量模型的特性、子特性和测量元进行质量定义和评价。

4.2 总体要求

4.2.1 功能要求

软件应实现以下核心功能：

——显示参数控制：支持分辨率、刷新率、亮度、对比度的调节；

——图像处理：支持色彩空间转换、图像缩放、Gamma 校正；

——人机交互：支持至少一种输入方式（如物理按键、触控、红外遥控），并能响应输入指令执行对应操作（如按键“+”触发亮度增加）；

——状态监测：实时监测显示面板温度（采样周期 $\leq 1\text{ s}$ ）、电源电压（采样周期 $\leq 100\text{ ms}$ ），超限时触发保护机制（如降低亮度）。

4.2.2 性能要求

4.2.2.1 实时性

显示帧数据刷新任务的响应延迟 $\leq 10\text{ ms}$ （从帧缓冲数据准备完成到开始输出的时间）；用户输入指令的响应时间 $\leq 100\text{ ms}$ （从指令接收至执行完成的时间）。

4.2.2.2 资源占用

满负载运行时，内存占用率 $\leq 70\%$ ，CPU使用率 $\leq 80\%$ ；

4.2.2.3 启动速度

软件从上电到首次显示图像的时间 $\leq 3\text{ s}$ （不含硬件初始化时间）。

4.2.3 兼容性要求

4.2.3.1 显示终端宜支持至少 3 种主流显示接口协议，如 MIPI-DSI（适用于中小尺寸屏幕）、LVDS（适用于液晶显示器）。

4.2.3.2 应支持至少一种主流嵌入式操作系统（如 Linux、FreeRTOS、RT-Thread）。

5 设计要求

5.1 架构设计

5.1.1 分层架构

软件应采用分层架构，至少包含以下三层：

——硬件抽象层（HAL）：封装显示面板、背光驱动、传感器等硬件的具体操作，提供统一的函数接口；同一类硬件（如不同型号的 LCD 面板）的接口函数名、参数应保持一致；

——核心服务层：实现显示控制的核心逻辑，包括：

- 显示参数管理：维护当前分辨率、刷新率等参数，提供参数查询与设置接口；
- 图像处理引擎：执行图像缩放、色彩校正等算法，处理延迟；
- 任务调度：基于优先级调度实时任务（如帧刷新）与非实时任务（如日志记录），实时任务优先级高于非实时任务。

——应用接口层：提供面向用户的功能接口，包括 API 函数和配置命令。

5.1.2 模块依赖

模块间的依赖关系应采用“单向依赖”原则，即上层模块可依赖下层模块，下层模块不得依赖上层模块。应禁止模块间形成循环依赖。

5.2 模块设计

5.2.1 驱动模块

驱动模块应包括但不限于：

——显示面板驱动：

- 支持面板初始化（含时序参数配置）、显示开启/关闭、分辨率切换等功能；初始化失败时应返回明确的错误码；
- 实现面板状态监测（如是否连接、是否正常工作）；

——背光驱动：

- 支持亮度调节，从最低亮度到最高亮度的切换时间 ≤ 500 ms；
- 具备过流保护逻辑，当检测到背光电流超过额定值120 %时，应在10 ms内关闭背光并记录故障。

5.2.2 图像处理模块

图像处理模块应包括：

——图像缩放：支持 bilinear、bicubic 等缩放算法，缩放后图像的峰值信噪比 ≥ 30 dB；

——色彩校正：支持白平衡调节、色域映射，校正后色彩误差（ ΔE ） ≤ 3 ；

——动态对比度：根据输入图像的亮度分布自动调整对比度，响应时间 ≤ 1 帧周期。

5.2.3 交互控制模块

5.2.3.1 输入解析

支持对物理按键（如电源键、音量键）、触控信号、红外遥控的解析，解析准确率 $\geq 99\%$ 。

5.2.3.2 指令执行

对解析后的指令进行权限校验（如“恢复出厂设置”需管理员权限），校验通过后执行对应操作，执行结果应反馈（如通过LED指示灯闪烁提示成功/失败）。

5.2.4 安全管理模块

5.2.4.1 权限管理

通过加密的权限密钥区分用户等级，密钥存储在硬件安全区。

5.2.4.2 固件校验

对加载的固件进行完整性校验和合法性校验，校验失败则拒绝加载。

5.3 接口设计

5.3.1 接口定义

模块间接口应通过文档明确以下内容：

——接口名称；

——输入参数：名称、数据类型、取值范围；

- 输出参数：名称、数据类型、含义；
- 返回值：错误码（如 0 表示成功，-1 表示参数无效）；
- 调用约束。

5.3.2 通信接口

与外部设备（如主控板、调试工具）的通信接口应满足：

- 采用校验机制：UART 通信采用“数据+校验和”格式，SPI/I²C 通信启用硬件 CRC 校验，数据传输错误率 $\leq 10^{-6}$ ；
- 超时处理：通信超时时间可配置（默认 100 ms），超时后应重试（重试次数 ≤ 3 次），仍失败则触发错误处理（如记录日志）。

5.4 代码设计

5.4.1 编码

5.4.1.1 编码规则宜按 GB/T 28169 的规定执行。

5.4.1.2 宜按照软件单元规范和编码规则开发软件。编码规则可以是众所周知的行业标准，也可以是制造商规定内部标准。宜按照软件单元规范和编码规则对代码进行审查。

注1：编码规则旨在限制编程的自由度，以避免程序代码变得难以理解。

注2：编码规则通常定义编程语言的子集或使用强类型编程语言（参见GB/T 20438.7—2017的C.4.1，C语言在关键系统中的使用指南（MISRA C））。

注3：关面向对象的体系架构和设计的指南，见GB/T20438.7—2017中的附录G。

注4：编码输出物宜包含源代码列表和代码审核报告。

5.4.1.3 宜使用以下编程手段来避免系统性失效：

- 变量和配置参数的范围检查和合理性检查；
- 时间和(或)逻辑程序时序监控，以检测有缺陷的程序时序；
- 限制全局变量的数量或范围。

5.4.1.4 为了限制网络安全风险，宜采用安全编码规则。

5.4.2 内存管理

5.4.2.1 动态内存分配宜指定最大尺寸，分配失败时应返回错误并处理。

5.4.2.2 动态分配的内存应在使用后释放，通过工具（如 Valgrind）检测无内存泄漏。

5.4.3 异常处理

5.4.3.1 对可能发生的异常（如空指针、数组越界、除法溢出）进行捕获和处理，避免程序崩溃。

5.4.3.2 异常发生时，应记录详细日志（包括异常类型、发生位置、时间戳）。

6 验证要求

6.1 验证流程

验证应遵循GB/T 8566-2022第6章要求，按以下阶段开展，前一阶段通过后方可进入下一阶段：

- 设计验证：验证设计文档的完整性、一致性；
- 代码验证：验证代码与设计的符合性、代码质量；
- 集成验证：验证模块间接口的正确性；
- 系统验证：验证软件整体功能、性能及安全性。

6.2 设计验证

6.2.1 文档审查

审查以下设计文档，审查人员应包括设计、测试、质量管理人员：

- 软件需求规格说明书：是否覆盖 4.2.1 的核心功能，需求描述是否清晰、可验证；
- 架构设计文档：分层架构是否符合 5.1.1 要求，模块划分是否满足高内聚、低耦合；

- 模块设计文档：模块功能是否明确，接口定义是否完整；
- 审查通过标准：文档应无重大缺陷（如功能遗漏、接口冲突），轻微缺陷（如表述不规范）整改率 100%。

6.2.2 模型检查

应对核心模块的逻辑模型进行检查，确保无死锁、无逻辑矛盾。

6.3 代码验证

6.3.1 静态代码分析

宜使用工具检测代码，应满足：

- 无高危缺陷（如缓冲区溢出）；
- 中危缺陷数量 ≤ 5 个/千行代码；
- 代码规范符合性 $\geq 95\%$ 。

6.3.2 单元测试

对每个模块开展单元测试，满足：

- 测试用例覆盖正常输入、边界输入（如亮度值 0 和最大值）、异常输入（如负数亮度值）；
- 所有测试用例执行通过（无失败）。

6.4 集成验证

6.4.1 接口测试

测试模块间接口的正确性，包括：

- 参数传递：验证输入参数在正常范围、边界值、异常值时，接口的处理是否符合设计；
- 数据交互：验证模块间传递的复杂数据（如图像帧）是否完整、无误；
- 异常场景：模拟接口调用超时、模块崩溃等场景，验证依赖模块的容错能力。

6.4.2 集成测试环境

应搭建硬件在环（HIL）测试环境，使用真实的显示终端硬件或等效模拟器，模拟实际运行时的硬件交互。

6.5 系统验证

6.5.1 功能验证

测试用例覆盖4.2.1的所有核心功能，每个功能点至少包含3个测试用例（正常场景、边界场景、异常场景）。

6.5.2 可靠性验证

6.5.2.1 稳定性测试

软件在额定工作条件下连续运行1000小时，记录故障次数，换算后持续稳定运行时间应不小于10000小时。

6.5.2.2 环境适应性

在高低温环境下各运行24小时，无崩溃、无功能异常。

6.5.3 安全性验证

6.5.3.1 权限测试

使用用户级权限尝试修改管理员级参数（如工厂校准数据），验证是否被拒绝。

6.5.3.2 固件防护

尝试加载未签名的固件，验证是否被拒绝；模拟固件传输过程中的数据篡改，验证是否能检测并拒绝加载。

6.5.3.3 漏洞扫描

使用工具检测已知漏洞（如缓冲区溢出、命令注入），无高危漏洞。

6.6 验证记录

所有验证活动应形成记录，包括：

- 验证计划：明确验证目标、范围、方法、人员及时间安排；
- 测试用例：包含编号、测试目的、输入、预期输出、实际输出；
- 缺陷报告：记录发现的缺陷（严重度、复现步骤、整改建议）及整改结果；
- 验证报告：汇总验证结果，明确是否通过验证。

7 文档管理要求

7.1 设计阶段文档

应包含以下文档：

- 软件需求规格说明书：描述软件的功能需求、性能需求、接口需求、环境需求；
- 架构设计文档：含架构图、分层说明、模块划分及模块间关系；
- 模块设计文档：每个模块的功能描述、接口定义、数据结构、状态机（如适用）；
- 接口规范文档：汇总所有模块间接口及外部通信接口的定义；
- 编码规范文档：明确命名规则、注释要求、代码格式等。

7.2 验证阶段文档

应包含以下文档：

- 验证计划：见 6.6 条要求；
- 测试用例集：按模块或功能分类，包含所有测试用例；
- 测试报告：按验证阶段（单元、集成、系统）分别编制，含测试结果、缺陷统计及分析；
- 缺陷跟踪表：记录缺陷 ID、描述、严重度、状态（未解决/已解决）、解决时间。

7.3 交付文档

软件交付时应提供以下文档：

- 用户手册：说明软件的功能、操作方法、常见问题排查；
- 维护手册：包含软件架构、模块功能、故障诊断流程、日志解析方法；
- 固件升级指南：说明升级工具、升级步骤、回滚方法及注意事项；
- 验证报告摘要：汇总系统验证的关键结果。

7.4 文档管理

7.4.1 文档版本号格式为“V 主版本号.次版本号”（如 V1.0），修改后次版本号递增（如 V1.1），重大修改主版本号递增（如 V2.0）。

7.4.2 文档应存储在安全的服务器或介质中，设置访问权限（如设计文档仅开发人员可修改）。

参 考 文 献

- [1] GB/Z 41912-2022 低压开关设备和控制设备 嵌入式软件开发指南
[2] GB/T 20438.7-2017 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述
-