



中华人民共和国国家标准

GB/T 33781—2017

可编程逻辑器件软件开发通用要求

General requirements for programmable logic device software development

2017-05-31 发布

2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语 1

 3.1 术语和定义 1

 3.2 缩略语 2

4 一般要求 2

 4.1 可编程逻辑器件软件生存周期框架 2

 4.2 完整性级别 3

 4.3 重用 3

 4.4 生产管理 3

 4.5 可靠性与安全性 3

 4.6 保密和病毒防护 3

5 详细要求 4

 5.1 系统需求分析 4

 5.2 软件需求分析 4

 5.3 设计 4

 5.4 实现 5

 5.5 确认测试 6

 5.6 验收与交付 6

 5.7 运行与维护 7

 5.8 配置管理 7

 5.9 质量保证 7

 5.10 纠正措施 7

 5.11 验证 7

 5.12 风险管理 8

 5.13 安全管理 8

 5.14 分包方管理 8

 5.15 与相关方的协调 8

附录 A（规范性附录） 可编程逻辑器件软件技术文档列表 9

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位：中国航天科工集团第三研究院第三〇四研究所、中国电子技术标准化研究院、上海计算机软件技术开发中心、国家卫星气象中心、中核控制系统工程有限公司。

本标准主要起草人：李艳志、于林宇、张津荣、刘军、王栋、朱琳、刘伟、王颖、张旻旻、张东胜、蔡立志、程朝晖、李朝历、李丽华、郑金艳、孟伟、张国宇、杨楠、张玉、陈磊、刘潇健、于秀明、车容俊、周鹏程、张志刚、张明敏。

可编程逻辑器件软件开发通用要求

1 范围

本标准规定了可编程逻辑器件软件开发过程的相关要求,规定了可编程逻辑器件软件开发过程全生存周期中每个阶段的目标、技术要求。

本标准适用于可编程逻辑器件软件的开发过程。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 11457—2006 信息技术 软件工程术语
GB/T 18492—2001 信息技术 系统和软件完整性级别
GB/T 20158—2006 信息技术 软件生存周期过程 配置管理
GB/T 33783—2017 可编程逻辑器件软件测试指南
GB/T 33784—2017 可编程逻辑器件软件开发文档编制规范

3 术语、定义和缩略语

3.1 术语和定义

GB/T 11457—2006 中界定的以及下列术语和定义适用于本文件。

3.1.1

可编程逻辑器件 programmable logic device
允许用户编程(配置)实现所需逻辑功能的器件。

3.1.2

复杂可编程逻辑器件 complex programmable logic device
由多个逻辑模块组合而成,并由可编程的连线进行连接,从而构成完整的逻辑电路的器件。

3.1.3

现场可编程门阵列 field programmable gate array
由可配置逻辑单元、输入输出模块和内部连线等组成的器件。

3.1.4

硬件描述语言 hardware description language
一种用来建模、设计和仿真硬件功能的语言。

3.1.5

可编程逻辑器件软件 programmable logic device software
针对 FPGA、CPLD 等可编程逻辑器件进行设计而产生的程序、文档和数据。

3.1.6

逻辑综合 synthesis
将设计输入转换成由基本逻辑单元组成的逻辑网表,根据约束条件对其优化并输出网表文件,供布

GB/T 33781—2017

局布线器进行实现的过程。

3.1.7

布局布线 place & route

利用逻辑综合生成的网表,结合指定的约束条件,生成配置文件的过程。

3.1.8

功能仿真 functional simulation

在不包含信号传输延时信息的条件下,用仿真方法验证设计的逻辑功能是否正确的过程。

3.1.9

门级仿真 gate-level simulation

通过仿真工具确认综合后功能及时序是否正确的过程。

3.1.10

时序仿真 timing simulation

在包含信号传输的门级延时和布线延时信息的条件下,用仿真方法验证布局布线后功能和时序是否正确的过程。

3.1.11

静态时序分析 static timing analysis

分析逻辑综合或布局布线后得到的静态时序信息,根据信息提示找出不满足建立/保持时间路径以及不符合约束路径的过程。

3.1.12

逻辑等效性检查 logic equivalence check

确认代码、网表间逻辑一致性的过程。

3.2 缩略语

下列缩略语适用于本文件。

CPLD 复杂可编程逻辑器件(Complex Programmable Logic Device)

FPGA 现场可编程门阵列(Field Programmable Gate Array)

HDL 硬件描述语言(Hardware Description Language)

IP 知识产权(Intellectual Property)

PLD 可编程逻辑器件(Programmable Logic Device)

PLDS 可编程逻辑器件软件(Programmable Logic Device Software)

PSCI 可编程逻辑器件软件配置项(PLD Software Configuration Item)

4 一般要求

4.1 可编程逻辑器件软件生存周期框架

4.1.1 基本活动

可编程逻辑器件软件开发过程中的基本活动包括:

- a) 系统需求分析;
- b) 软件需求分析;
- c) 设计;
- d) 实现;
- e) 确认测试;

- f) 验收与交付;
- g) 运行与维护。

4.1.2 管理活动

可编程逻辑器件软件开发过程中的管理活动包括:

- a) 配置管理;
- b) 风险管理;
- c) 分包方管理;
- d) 安全性管理。

4.1.3 支持活动

可编程逻辑器件软件开发过程中的支持活动包括:

- a) 质量保证;
- b) 纠正措施;
- c) 验证;
- d) 与第三方评测机构的联系;
- e) 与相关开发方的协调。

4.2 完整性级别

应按 GB/T 18492—2001 确定可编程逻辑器件软件的完整性级别,并按照该等级进行分级管理。

4.3 重用

应制定软件重用管理相关要求,一般应包括:

- a) 重用软件的开发和使用原则;
- b) 使用重用软件前应对其适用性进行分析评估,评估结果需进行审查和确认,必要时可补充测试。

4.4 生产管理

可编程逻辑器件芯片和配置芯片应按规定选用合格的生产厂和指定产品,可编程逻辑器件软件产品的贮存与管理包括:

- a) 可编程逻辑器件软件复制、固化应在质量管理部门的监督下,指定专人,按照操作规程在指定(或专用)设备上,并记录可编程逻辑器件软件复制、固化过程;
- b) 复制、固化用的母盘应由产品库提供;
- c) 复制、固化前应对设备进行检查;
- d) 复制、固化后做好检验、包装和标记,验证合格后方可交付。

4.5 可靠性与安全性

应根据关键等级,在开发各阶段,从系统、硬件和软件等方面对影响安全性与可靠性的因素进行分析,开展安全性可靠性相关需求的分析、设计、实现,并开展验证,确保安全性与可靠性。

4.6 保密和病毒防护

保密和病毒防护应贯穿可编程逻辑器件软件全生存周期。开发单位应针对可编程逻辑器件和开发环境进行保密安全性分析,找出可能存在的漏洞,制定并落实相应的防护措施。

5 详细要求

5.1 系统需求分析

开发方应参与需方组织的 PSCI 所属系统的需求分析活动,明确所在系统对 PSCI 的需求,系统需求分析一般应包括以下内容:

- a) 针对器件可获得性、开发便利性、功耗、时钟频率、芯片资源、抗状态翻转、器件等级、封装方式、工作环境(含温度)、存储温度、辐照总剂量等系统要求开展必要性与可行性分析;开展风险分析,确认风险项并制定对应的预防措施和应急响应,形成可行性及风险分析报告;
- b) 明确关键等级,必要时为每个功能确定安全关键等级;
- c) 明确功能、性能、接口、功耗、降额、工作条件等技术指标;
- d) 明确外部接口的通信协议、电气特性、时序特性等与可编程逻辑器件相关的软件/硬件接口;
- e) 提出安全性和可靠性要求,如结构、算法、容错、冗余、抗状态翻转等;
- f) 明确关键算法的算法方程和技术指标;
- g) 明确 HDL 语言和设计方法约束;
- h) 提出资源、时序等余量要求;
- i) 提出固化、工作环境要求;
- j) 提出实时性、可测试性要求;
- k) 提出 IP 核使用要求;
- l) 提出安全保密性、重用、进度、验收与交付、运行与维护、配置管理、质量保证等要求;
- m) 提出测试级别、测试内容、测试充分性等测试要求。

5.2 软件需求分析

开发方应依据开发技术要求等相关文件,明确每项需求得以满足所使用的方法,建立与系统需求的追踪关系,需求分析一般应包括以下内容:

- a) 定义功能、性能、接口、管脚分配及约束等需求;
- b) 开展安全性与可靠性分析,确定安全性与可靠性需求,明确抗状态翻转等技术方法;
- c) 必要时,开展算法原型仿真分析;
- d) 确定开发环境、工具及版本;
- e) 确定芯片型号、等级约束和封装形式;
- f) 确定 HDL 语言和设计方法约束;
- g) 确定资源、时序等余量需求;
- h) 确定固化、工作环境需求;
- i) 确定实时性、可测试性需求;
- j) 确定 IP 核使用需求;
- k) 确定安全保密性、重用、进度、配置管理、质量保证、测试等需求;
- l) 必要时,明确与软件相关的地址分配;
- m) 定义实现系统需求产生的派生需求,对其单独标识并反馈至系统需求分析过程,评估派生需求对系统需求分析的影响。

5.3 设计

5.3.1 结构设计

开发方应在结构设计过程定义和记录 PLDS 结构,标识组成 PLDS 的单元及接口,建立与需求的追

踪关系,结构设计一般应包括以下内容:

- a) 确定 PLDS 结构及单元划分,定义单元及单元间的关系,描述单元的功能、性能、接口,确保全部需求分配至相应单元;
- b) 描述单元间的数据流和控制流;
- c) 描述结构及单元的设计思路;
- d) 必要时,应通过仿真和分析验证结构设计是否满足要求;
- e) 确定时钟、复位方案;
- f) 根据安全性和可靠性需求,开展安全性、可靠性设计;
- g) 完成算法由抽象层次到实现层次的转换,确定算法的输入、输出接口,描述算法的实现过程,必要时对中间参数进行描述;
- h) 开展验证方案设计;
- i) 结构设计过程中产生的派生需求应反馈至需求分析过程并评估影响;
- j) 重新评估可行性和风险。

5.3.2 详细设计

开发方应依据结构设计详细描述 PLDS 的单元并可作为软件实现的依据,建立与结构设计的追踪关系,一般应包括以下内容:

- a) 对各单元进行详细说明,包含各单元地址分配、控制方式、接口、存储器空间、时序说明、性能指标、测试要求等内容;
- b) 描述各单元的设计原理和所采用的技术方法及过程;
- c) 详细说明各单元在实现时采用的设计输入方法;
- d) 必要时,列出厂商、版本等 IP 核属性;
- e) 完善安全性、可靠性设计,并分析详细设计是否符合安全性与可靠性设计要求;
- f) 完善验证方案设计;
- g) 应标识出未被使用的功能并评估其对安全性的影响;
- h) 约束软件的设计、固化和操作,若存在无约束的情况,应评估其对安全性的影响并标识;
- i) 详细设计过程中产生的派生需求应反馈至结构设计过程或其他过程并评估影响。

5.4 实现

5.4.1 编码

开发方应依据设计开展编码活动,形成源代码或电路器件连接原理图。

5.4.2 仿真测试环境设计与实现

开发方应编制仿真测试计划和仿真测试说明,并依据仿真测试说明设计仿真测试环境,编制仿真测试向量集。

5.4.3 功能仿真

开发方应对源代码或原理图开展单元级别和配置项级别功能仿真,执行测试用例。必要时,应通过统计语句、分支、状态机等覆盖率信息保证仿真测试的充分性。测试级别、测试方法定义见 GB/T 33783—2017。

5.4.4 综合与布局布线

开发方应在完成编码与功能仿真后开展综合与布局布线,完善设计说明。

GB/T 33781—2017

5.4.5 网表验证

开发方针对布局布线后网表应开展时序仿真、静态时序分析,必要时,应开展综合后门级仿真和逻辑等效性检查。

5.4.6 分析和记录

开发方应在仿真测试报告中记录仿真测试及分析的结果。

5.4.7 修改和回归测试

开发方应根据仿真测试的结果对软件进行修改,开展回归测试并根据需要更新文档和相关产品。

5.4.8 固化

开发方应将可烧录文件固化在可编程逻辑器件芯片或配置芯片中。

5.5 确认测试

5.5.1 测试的独立性

负责开展确认测试的人员不应是从事该 PLDS 设计和实现的人员,可以由第三方评测机构开展。

5.5.2 测试环境

应在真实的目标板、系统或在需方批准的替代环境上开展配置项级或系统级确认测试。

5.5.3 测试准备

应编制确认测试计划、确认测试说明,识别被确认的每项需求,设计测试用例。

5.5.4 测试执行

应通过确认测试对每项 PLDS 需求进行确认,分析实际结果与期望结果的差异,明确需求与确认行为及结果之间的可追踪性。对于某些无法通过测试实施确认的特性或需求,经需方认可,可采用分析、审查、评审等方式开展确认并将结论纳入确认测试报告。

5.5.5 修改和回归测试

应根据确认测试的结果对软件进行修改并开展回归测试并根据需要更新文档和其他产品。

5.5.6 分析和记录

应在确认测试报告中记录测试及分析的结果。

5.6 验收与交付

5.6.1 验收和评审

开发方应按照开发技术要求或合同规定向需方提出验收申请,为需方开展验收测试、评审提供支持并记录结果,编写使用说明,按开发技术要求或合同要求准备开发总结报告等文档用于验收与交付,文档具体格式要求见 GB/T 33784—2017。

5.6.2 产品交付

开发方按照开发技术要求或合同规定向需方交付产品。

5.6.3 培训与支持

开发方按照开发技术要求或合同规定为需方提供必要的培训与支持。

5.7 运行与维护

交付与验收后,开发方应按照开发技术要求或合同规定实施维护,以消除缺陷或满足需求变更,并做好技术状态控制、配置管理、回归测试和评审等工作。

5.8 配置管理

开发方应在开发过程中实施配置管理,具体要求见 GB/T 20158—2006。PLDS 配置管理项一般包括:

- a) 开发文档,文档列表见附录 A,具体内容和格式要求见 GB/T 33784—2017;
- b) 工程文件,见附录 A,包含设计输入、约束文件、综合和布局布线后产生的相关文件,采用工具进行三模冗余设计的,应包含三模前和三模后的工程文件;
- c) 开发工具、开发环境、测试工具、测试环境、问题/更改报告等。

5.9 质量保证

开发方应在开发过程中实施质量保证,一般应包括以下内容:

- a) 应按照计划对开发活动和工作产品定期地或事件驱动地进行评审或审核;
- b) 应保证合同、开发技术要求中要求的每项工作产品都存在,并对其开展评价、测试和纠正措施;
- c) 应按照 5.10 要求处理发现的问题;
- d) 负责质量保证的人员应具有资源、职责、权限和组织上的独立性,保证能客观开展质量保证评价并启动和验证纠正措施;
- e) 开发方应为每个质量保证活动准备并保存记录,记录应在合同期内保留。

5.10 纠正措施

5.10.1 问题/更改报告

开发方应编写问题/更改报告,说明在置于项目级或更高级配置控制下的 PLDS 的每一个问题,以及在合同、开发技术要求等描述的开发活动中的每一个问题。问题/更改报告应描述问题,所需的纠正措施和至今已采取的纠正措施,并作为纠正措施系统的输入信息。

5.10.2 纠正措施系统

开发方应建立纠正措施系统,以处理置于项目级或更高级配置控制下的 PLDS 中的每一个问题,以及在合同、开发技术要求、开发计划等描述的开发活动中的每一个问题,该系统应满足:

- a) 输入信息应由问题/更改报告组成;
- b) 应确保问题能及时报告并进入该系统,纠正工作得以启动并且问题得到解决,状态得以跟踪,并且问题记录在合同期内得以保持,形成闭环系统;
- c) 分析问题并预测其趋势;
- d) 对纠正措施进行评价,以确定问题是否得到解决、不利趋势是否得到扭转,更改是否正确实现且未引起其他问题。

5.11 验证

开发方应对系统需求分析、需求分析、设计、实现、确认测试过程进行验证,要求如下:

- a) 系统需求分析:复核可行性及风险分析、关键等级、安全性可靠性要求等,对可行性及风险分析报告和开发技术要求等相关文件开展评审;
- b) 可编程逻辑器件软件需求分析:分析需求和开发技术要求的可追踪性,审查需求及其变更情况,对需求规格说明等相关文件开展评审;
- c) 可编程逻辑器件软件设计:确认设计说明与需求规格说明、开发技术要求的一致性,对设计说明等相关文件开展评审;
- d) 可编程逻辑器件软件实现:开展功能仿真、时序仿真、静态时序分析,必要时开展门级仿真、逻辑等效性检查,对仿真测试开展评审;
- e) 确认测试:应保证确认测试覆盖所有任务要求和所有需求,对确认测试开展评审;
- f) 验收与交付:需方应组织对验收开展测试和评审。

5.12 风险管理

开发方应在整个开发过程中进行风险管理,一般应包括以下内容:

- a) 制定风险管理计划;
- b) 标识、分析和排序项目中潜在的技术、成本和进度风险;
- c) 制定管理风险的策略;
- d) 实施风险管理策略,跟踪和控制风险。

5.13 安全性管理

开发方应按照合同规定的保密、安全要求开发产品并实施相应管理。

5.14 分包方管理

如果有分包方,开发方应将本标准的技术要求及必要的主合同要求纳入与分包方签订的子合同,确定并实施验证或其他必要的活动,以确保分包方开发的产品满足规定的要求。

5.15 与相关方的协调

开发方应按照本标准的技术要求及合同规定与相关方进行协调。

注:相关方指在同一个或有关的系统中承担与本 PSCI 相关的其他开发工作的组织,不包括分包方。

附 录 A
(规范性附录)
可编程逻辑器件软件技术文档列表

可编程逻辑器件软件的技术文档列表见表 A.1。

表 A.1 可编程逻辑器件软件技术文档列表

序号	过程	文档名称
1	系统需求分析	可行性和风险分析报告
		开发技术要求
2	需求分析	需求规格说明
3	设计	设计说明
4	实现	仿真测试计划
5		仿真测试说明
6		仿真测试报告
7		工程文件
8	确认测试	确认测试计划
9		确认测试说明
10		确认测试报告
11	验收与交付	开发总结报告
12		使用说明

中 华 人 民 共 和 国
国 家 标 准
可编程逻辑器件软件开发通用要求
GB/T 33781—2017

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1 字数 22 千字
2017年6月第一版 2017年6月第一次印刷

*

书号: 155066·1-56971 定价 18.00 元



GB/T 33781—2017