ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

ПНСТ 118 — 2016/ МЭК 62566: 2012

АТОМНЫЕ СТАНЦИИ

Контроль и управление, важные для безопасности. Использование программируемых интегральных схем для применения в системах, выполняющих функции категории А

(IEC 62566:2012, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 45

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 322 «Атомная техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 июня 2016 г. № 40-пнст

4 Настоящий стандарт идентичен международному стандарту МЭК 62566:2012 «Атомные станции. Контроль и управление, важные для безопасности. Использование программируемых интегральных схем для применения в системах, выполняющих функции категории А» (IEC 62566:2012 «Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions», IDT)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные и межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА.

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 9 мес до истечения срока его действия разработчику настоящего стандарта по адресу: gost.e-ecolog.ru *в Федеральное агентство по техническому регулированию и метрологии по адресу: Ленинский просп., д. 9, Москва В-49, ГСП-1, 119991.*

*В случае отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты» и журнале «Вестник технического регулирования». Уведомление будет размещено также на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
1.1 Общие положения 1
1.2 Применение настоящего стандарта 2
2 Нормативные ссылки 2
3 Термины и определения 3
4 Обозначения и сокращения 5
5 Общие требования к проектам HDL-программируемых устройств 5
5.1 Общие положения 5
5.2 Жизненный цикл 5
5.3 Управление проектом HDL-программируемого устройства 8
5.4 План обеспечения качества HDL-программируемого устройства 8
5.5 Управление конфигурацией 8
6 Спецификация требований к HDL-программируемому устройству 9
6.1 Общие положения 9
6.2 Функциональные аспекты спецификации требований 9
6.3 Детерминированное проектирование 10
6.4 Обнаружение отказов и устойчивость к неисправностям 10
6.5 Определение требований с помощью инструментов проектирования на уровне электронных систем 10
6.6 Анализ и обзор требований 11
7 Процесс обоснования применения для программируемых интегральных схем, конфигурируемых блоков и предварительно разработанных блоков 11
7.1 Общие положения 11
7.2 Спецификация требований к элементам 12
7.3 Правила использования 12
7.4 Выбор 13
7.5 Подтверждение обоснования применения 14
7.6 Модификация для обоснования применения 14
7.7 Модификация после обоснования применения 14
7.8 Документация для обоснования применения 14
8 Проектирование и реализация HDL-программируемого устройства 15
8.1 Общие положения 15
8.2 Языки описания аппаратуры и сопутствующие инструменты 15
8.3 Проектирование 15
8.4 Реализация 19
8.5 Инструменты системного уровня и автоматизированного кода 21
8.6 Документация 22
8.7 Экспертиза проекта и реализации 22
9 Верификация HDL-программируемого устройства 23
9.1 Общие положения 23
9.2 План верификации 23
9.3 Верификация использования предварительно разработанных элементов 24
9.4 Верификация проекта и реализации 24
9.5 Испытательные стенды 24

9.6 Тестовое покрытие 25
9.7 Выполнение испытаний. 25
9.8 Статическая верификация 26
10 Аспекты системной интеграции HDL-программируемого устройства 26
10.1 Общие положения 26
10.2 Аспекты плана системной интеграции для HDL-программируемого устройства 26
10.3 Специфические аспекты системной интеграции 27
10.4 Верификация интегрированной системы 27
10.5 Процедуры устранения отказа 28
10.6 Аспекты отчета об испытании интегрированной системы с HDL-программируемым устройством 28
11 Аспекты валидации системы с HDL-программируемыми устройствами 28
11.1 Общие положения 28
11.2 Аспекты плана валидации системы с HDL-программируемыми устройствами 28
11.3 Валидация системы. 28
11.4 Аспекты отчета о валидации системы с HDL-программируемыми устройствами 29
11.5 Процедуры устранения отказа 29
12 Модификация 29
12.1 Модификация требований, конструкции или реализации 29
12.2 Модификация микроэлектронной технологии. 29
13 Производство HDL-программируемого устройства 30
13.1 Общие положения 30
13.2 Производственные испытания 30
13.3 Программирующие файлы и программирование 30
14 Аспекты монтажа, ввода в эксплуатацию и эксплуатации HDL-программируемого устройства . . . 30
15 Инструментальные программы для разработки HDL-программируемых устройств. 31
15.1 Общие положения 31
15.2 Дополнительные требования к инструментам проектирования, реализации и моделирования 31
16 Сегментация или разделение конструкции 31
16.1 Вводные сведения 31
16.2 Вспомогательные функции или функции поддержки 32
17 Защита от отказа по общей причине в HDL-программируемом устройстве 32
17.1 Вводные сведения 32
17.2 Требования. 33
Приложение А (справочное) Документация. 34
Приложение В (справочное) Разработка HDL-программируемых устройств 36
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 39
Библиография 40

Введение

a) Технические положения, основные вопросы и организация стандарта

Используемые на атомных станциях (далее — АС) электронные системы класса 1 (по МЭК 61513), необходимые в аварийных ситуациях, должны быть аттестованы до начала их эксплуатации.

В традиционных системах, которые являются компьютерными, можно провести разделение между аппаратной и программной частями. Аппаратные средства в основном проектируют с применением стандартизированных элементов, имеющих заданные электронные функции, таких как микропроцессоры, таймеры или сетевые контроллеры, тогда как программное обеспечение применяется для координации работы различных частей аппаратных средств и реализации прикладных функций.

В настоящее время проектировщики средств контроля и управления могут создавать прикладные функции непосредственно на одной интегральной схеме с помощью таких устройств, как программируемая пользователем вентильная матрица (ППВМ), или устройств, изготовленных по подобным технологиям. Функция такой интегральной схемы определяется не поставщиком физического элемента или микроэлектронной технологии, а проектировщиком средств контроля и управления.

Настоящий стандарт рассматривает интегральные схемы (ИС):

1) основанные на предварительно разработанных микроэлектронных ресурсах;

2) разработанные в рамках проекта по контролю и управлению;

3) разработанные с помощью языков описания аппаратуры (HDL) и связанных с ними инструментов, используемых для реализации требований в надлежащей сборке предварительно разработанных микроэлектронных ресурсов.

Данные схемы называют «HDL-программируемыми устройствами» (HPD). Операторы HDL, описывающие HPD, могут включать в себя создание экземпляров предварительно разработанных блоков (PDB), которые, как правило, поставляются в виде библиотек, макроопределений или IP-ядер.

HPD могут представлять собой эффективные решения для реализации функций, требуемых проектом по контролю и управлению (I&C). Однако верификацию и валидацию (V&V) могут ограничивать такие проблемы, как большое число внутренних путей и ограниченная наблюдаемость, если HPD разрабатывалось без учета верифицируемости.

Для того чтобы достигнуть уровня надежности, требуемого для систем контроля и управления по обеспечению безопасности, разработка HPD должна соответствовать строгим технологическим и техническим требованиям, таким как требования, приведенные в настоящем стандарте, включая спецификацию требований, выбор заготовок интегральных схем и предварительно разработанных блоков (PDB), проектирование и реализацию, верификацию и методики эксплуатации и технического обслуживания.

Настоящий стандарт предназначен для использования проектировщиками аппаратных средств, операторами АС (энергетическими компаниями) и регулирующими органами. Регулирующие органы могут воспользоваться рекомендациями по оценке важных аспектов, таких как проектирование, реализация, верификация и валидация HPD.

b) Место настоящего стандарта в структуре серии стандартов МЭК ПК 45А

МЭК 61513 является документом МЭК ПК 45А первого уровня и содержит руководство, применимое к контролю и управлению на уровне системы. МЭК 61513 дополнен руководством на аппаратном уровне (МЭК 60987) и уровне программного обеспечения (МЭК 60880 и МЭК 62138). МЭК 62340 содержит требования, направленные на снижение и предотвращение возможности отказа по общей причине функций категории А.

МЭК 62566 является документом МЭК ПК 45А второго уровня, который устанавливает мероприятия, проводимые при разработке HDL-программируемых устройств. МЭК 62566 дополняет МЭК 60987, который рассматривает типовые проблемы проектирования аппаратуры компьютерных систем. По вопросам решения проблем, идентичных проблемам разработки программного обеспечения, данный стандарт ссылается на МЭК 60880.

Более подробное описание структуры серии стандартов МЭК ПК 45А см. в перечислении d) настоящего введения.

c) Рекомендации и ограничения относительно применения стандарта

Важно отметить, что настоящий стандарт не устанавливает дополнительных функциональных требований к системам безопасности.

Особые требования и рекомендации разработаны по следующим аспектам:

1) подход к определению требований к проектированию, реализации и верификации HPD (см. 3.7) и управлению соответствующими аспектами интеграции на уровне систем и валидации;

2) подход к анализу и выбору заготовок интегральных схем, микроэлектронных технологий и PDB (см. 3.11), используемых при разработке HPD;

3) методики управления модификацией и конфигурацией HPD;

4) требования к выбору и использованию программных инструментов, применяемых при разработке HPD.

Цифровые технологии продолжают быстро развиваться, поэтому в настоящем стандарте невозможно рассмотреть все современные технологии и методики проектирования.

Для гарантии того, что настоящий стандарт останется актуальным в будущем, особое внимание уделено принципиальным вопросам, а не конкретным технологиям. При разработке новых методик необходимо наличие возможности оценить пригодность таких методик посредством применения принципов безопасности, приведенных в настоящем стандарте.

d) Описание структуры серии стандартов МЭК ПК 45А и их связи с другими документами МЭК и документами других организаций (МАГАТЭ, ИСО)

Стандартом высшего уровня в серии стандартов МЭК ПК 45А является МЭК 61513. Он содержит общие требования к системам и оборудованию контроля и управления, выполняющим функции, важные для безопасности на атомных электростанциях. МЭК 61513 формирует структуру серии стандартов МЭК ПК 45А.

МЭК 61513 содержит прямые ссылки на другие стандарты МЭК ПК 45А, рассматривающие общие темы, связанные с классификацией функций и классификацией систем, аттестацией, разделением систем, защитой от отказа по общей причине, аспектами программного обеспечения ЭВМ, аспектами аппаратных средств ЭВМ и проектированием пультовых. Стандарты второго уровня, на которые имеются ссылки, последовательно рассматривают вместе с МЭК 61513.

На третьем уровне стандарты МЭК ПК 45А, на которые нет прямых ссылок в МЭК 61513, — это стандарты, связанные с определенным оборудованием, техническими методами или определенной деятельностью. Как правило, документы, ссылающиеся на документы второго уровня (по общим темам), могут использоваться самостоятельно.

Четвертый уровень серий стандартов МЭК ПК 45А представляет собой Технические Отчеты, которые не являются нормативными документами.

МЭК 61513 выполнен в формате изложения, подобном основной публикации по безопасности МЭК 61508, и содержит полную схему жизненного цикла безопасности и структуру жизненного цикла системы, а также предоставляет интерпретацию основных требований, изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4, применительно к ядерной отрасли. Соответствие МЭК 61513 облегчит выполнение требований, изложенных в МЭК 61508, поскольку они были интерпретированы для ядерной промышленности. В этой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 применительно к ядерной отрасли.

МЭК 61513 ссылается на стандарты ИСО и документ МАГАТЭ GS-R-3 и МАГАТЭ GS-G-3.1 по вопросам, связанным с обеспечением качества.

Стандарты серии МЭК ПК45А последовательно внедряют и детализируют принципы и основные аспекты безопасности, предусмотренные в Руководствах МАГАТЭ по безопасности атомных станций и в других документах по безопасности МАГАТЭ, в особенности в требованиях NS-R-1, устанавливающих требования к безопасности при проектировании атомных электростанций, и в Руководстве по Безопасности NS-G-1.3, рассматривающем системы контроля и управления, важные для безопасности на атомных электростанциях. Терминология и определения, используемые в стандартах ПК 45А, соответствуют терминам и определениям, используемым МАГАТЭ.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

АТОМНЫЕ СТАНЦИИ

Контроль и управление, важные для безопасности.

Использование программируемых интегральных схем для применения в системах, выполняющих функции категории А

Nuclear power plants. Instrumentation and control important to safety.
Development of HDL-programmed integrated circuits for systems performing category A functions

Срок действия — с 2017—04—01
по 2018—03—31

1 Область применения

1.1 Общие положения

Настоящий стандарт устанавливает требования к разработке высоконадежных HPD, применяемых в системах I&C (в ОПБ-88/97 используются следующие термины: «управляющие системы нормальной эксплуатации», «управляющие системы безопасности» и «управляющие системы, важные для безопасности») АС, выполняющих функции безопасности категории А согласно классификации по МЭК 61226.

Программирование HPD базируется на языках описания аппаратуры и сопутствующих программных инструментах. Они, как правило, основаны на заготовках программируемой пользователем вентильной матрицы или подобных микроэлектронных технологиях. Универсальные интегральные схемы, такие как микропроцессоры, не являются HPD.

Настоящий стандарт устанавливает требования к:

a) специализированному жизненному циклу разработки, включающему в себя все этапы разработки HPD, такие как разработка спецификации требований, проектирование, реализацию, верификацию, интеграцию и валидацию;

b) планированию и дополнительным мероприятиям, таким как модификация и производство;

c) выбору предварительно разработанных элементов, включающих в себя микроэлектронные ресурсы, такие как заготовка программируемой пользователем вентильной матрицы или программируемая логическая интегральная схема, и операторы HDL, представляющие собой PDB;

d) использованию принципов простоты и детерминистских принципов, признанных первостепенно важными для достижения «безотказной» реализации функций категории А;

e) инструментам для проектирования, реализации и HPD.

Настоящий стандарт не устанавливает требований к разработке микроэлектронных ресурсов, которые доступны как «серийные готовые» изделия и не разработаны по стандартам обеспечения качества на ядерных установках. Настоящий стандарт рассматривает разработки, выполненные с использованием данных микроэлектронных ресурсов в проекте по I&C с помощью HDL и сопутствующих инструментов.

Настоящий стандарт содержит рекомендации, позволяющие в максимально возможной степени избежать скрытых дефектов, остающихся в HDL-программируемых устройствах, и снизить восприимчивость к единичным отказам, а также к потенциальным отказам по общей причине. Установленные

Издание официальное

настоящим стандартом требования четкой и полной документации позволяют более эффективно применять МЭК 62340.

В настоящем стандарте не рассматриваются аспекты надежности, связанные с аттестацией по условиям внешней среды и отказами, обусловленными старением или физической деградацией. Данные вопросы рассмотрены в других стандартах, в частности в МЭК 60987, МЭК 60780 и МЭК 62342.

МЭК 60880:2006 (подраздел 5.7) содержит требования к защищенности, применимые к разработке HPD.

1.2 Применение настоящего стандарта

Настоящий стандарт содержит рекомендации и требования, необходимые для создания верифицируемых конструкций и реализаций, если требуется обоснование, например, для выполняемой функции или важности ее поведения в отношении безопасности. Системы I&C класса 1 могут использовать HPD, для которых не обязательно полное подтверждение соответствия требованиям настоящего стандарта, например в случае, если они не реализуют логику функции безопасности. Однако отклонения от требований настоящего стандарта следует обосновать.

Настоящий стандарт устанавливает мероприятия по разработке HPD, реализуемые в рамках специализированного жизненного цикла. Также в настоящем стандарте приведены мероприятия и рекомендации в дополнение к требованиям МЭК 61513 для интеграции на уровне систем и валидации в случае, если в конструкцию включены HPD.

Требования МЭК 60987, относящиеся к разработке программируемых логических устройств, применяют в дополнение к требованиям настоящего стандарта в случае, если HPD являются частью системы I&C класса 1.

Примечание — В случае противоречивых требований настоящий стандарт заменяет требования МЭК 60987 в отношении HPD класса 1.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие документы. Для датированных ссылок применяют только указанное издание ссылочного документа. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

IEC 60671, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing (МЭК 60671 Атомные электростанции. Системы контроля и управления, важные для безопасности. Испытания для проверки работоспособности)

IEC 60880:2006, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions (МЭК 60880:2006 Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А)

IEC 60987:2007, Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems (МЭК 60987:2007 Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения для компьютерных систем)

IEC 61513:2011, Nuclear power plants — Instrumentation and control important to safety — General requirements for systems (МЭК 61513:2011 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования)

IEC 62138, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (МЭК 62138 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В или С)

IEC 62340, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF) (МЭК 62340 Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине)

IAEA guide NS-G-1.3:2002, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants (Руководство МАГАТЭ NS-G-1.3:2002, Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

специализированная интегральная схема; СИС (application Specific Integrated Circuit; ASIC): Интегральная схема, спроектированная для решения конкретной задачи.

[IEC 60050-521:2002, статья 521-11-18]

Примечание — Специализированная интегральная схема разработана для целей одной компании. Она включает в себя заказные функции, определенные данной компанией.

3.2 **блок** (block): Одна из частей, составляющих конструкцию; блок может быть разделен на другие блоки.

Примечание — Блок представляет собой либо PDB, либо конфигурируемый блок, либо блок, разработанный во время рассматриваемого проекта.

3.3

отказ по общей причине; ООП[1)] (Common Cause Failure; CCF): Отказ двух или более систем или элементов вследствие единичного конкретного события или единичной конкретной причины.

[IAEA Safety Glossary, издание 2007 г.]

Примечание — Общие причины отказа могут быть внутренними или внешними по отношению к системе I&C.

[IEC 61513]

3.4 **уровень электронной системы;** ESL (ElectroniОПс System Level; ESL): Высокоуровневое описание электронной системы, основанное на наборе процессов, представляющих функциональность элементов, таких как микропроцессоры, память, специализированные вычислительные блоки или каналы связи.

Примечание — Настоящее описание позволяет проектировщику разделить систему на элементы, оценивать ее эксплуатационные характеристики при различном отображении функций на элементы и устанавливать требования к элементам.

Как правило, это выполняют с помощью таких языков, как SystemC (IEEE 1666), SystemVerilog (IEEE 1800) или Matlab (R).

3.5 **программируемая пользователем вентильная матрица;** ППВМ (Field Programmable Gate Array; FPGA): Интегральная схема, которая может быть запрограммирована в производственных условиях изготовителем средств I&C. Она включает в себя программируемые логические блоки (комбинационные и последовательностные), программируемые взаимосвязи между ними и программируемые блоки для ввода и/или вывода сигналов. Затем функцию определяет проектировщик контроля и управления, а не поставщик интегральных схем.

Примечание — Программируемые пользователем вентильные матрицы по своей сути являются цифровыми устройствами, но некоторые из них могут включать в свой состав аналоговые входы/выходы и аналого-цифровые преобразователи. FPGA могут включать в себя новейшие цифровые функции, такие как аппаратные умножители, собственную память и встроенные ядра процессора.

3.6 **язык описания аппаратуры;** HDL (Hardware Description Language; HDL): Язык, используемый для формального описания функций и/или структуры электронного элемента для документации, моделирования или синтеза.

Примечание — Наиболее широко используемые языки описания аппаратуры — это VHDL (IEEE 1076) и Verilog (IEEE 1364).

[1)] Принятое в ОПБ 88/97 определение «отказ по общей причине» — отказы систем (элементов), возникающие вследствие одного отказа, или ошибки персонала, или внешнего или внутреннего воздействия, или иной внутренней причины.

3.7 **HDL-программируемое устройство;** HPD (HDL-Programmed Device; HPD): Интегральная схема, конфигурируемая (для систем контроля и управления АС) с помощью языков описания аппаратуры и сопутствующих программных инструментов.

Примечание 1 — Языки HDL и сопутствующие инструменты (например, симулятор, синтезатор) используют для реализации требований в надлежащей сборке предварительно разработанных микроэлектронных ресурсов.

Примечание 2 — При разработке HPD можно использовать PDB.

Примечание 3 — HPD, как правило, основаны на заготовках FPGA, программируемой логической интегральной схемы (PLD) или подобных микроэлектронных технологиях.

3.8 **модуль** (module): Одна из частей, составляющих конструкцию; модуль можно разделить на другие модули.

Примечание — Термин «модуль» является синонимом термина «блок»; термин «блок» часто используют в контексте электронного проектирования. Термин «модуль», используемый в МЭК 60880, применяют в настоящем стандарте для ссылок на МЭК 60880.

3.9 **конфигурируемый блок** (native block): Блок, который представляет собой существовавший ранее ресурс в интегральной схеме (например, логическая схема или более сложный блок, такой как умножитель или контроллер последовательной передачи). Посредством программирования HPD блоки конфигурируют и связывают для обеспечения необходимой функции.

3.10 **список связей** (netlist): Описание электронного элемента с точки зрения взаимосвязей между его терминальными элементами (например, конфигурируемыми блоками).

3.11 **предварительно разработанный блок;** PDB (Pre-Developed Block; PDB): Предварительно разработанный функциональный блок, пригодный для описания на HDL.

Примечание 1 — PDB, как правило, поставляются в виде библиотек, макроопределений или IP-ядер. Их используют при разработке HPD и включают в это HPD.

Примечание 2 — PDB может потребовать значительных трудозатрат до его включения в HPD, например синтеза электронной схемы из операторов HDL, отображения условных элементов этой схемы на аппаратных структурах физической интегральной схемы и трассировки соединений.

3.12

предварительно разработанное программное обеспечение; PDS (Pre-Developed Software; PDS): Часть программного обеспечения, которая уже существует, доступна в качестве коммерческой или патентованной программы и предполагается к использованию.

[IEC 60880, пункт 3.28, модифицировано]

3.13

программируемая логическая интегральная схема; ПЛИС (Program-mable Logic Device; PLD): Интегральная схема, состоящая из логических элементов с рисунком схемных соединений, части которой программирует пользователь.

[IEC 60050-521:2002, статья 521-11-01]

Примечание 1 — Существуют различные виды программируемых логических интегральных схем, например стираемая программируемая логическая интегральная схема или сложная программируемая логическая интегральная схема (CPLD).

Примечание 2 — Различия между FPGA и PLD не определены четко, но ПЛИС обычно относится к более простому устройству, чем FPGA.

3.14 **уровень регистровых передач;** RTL (Register Transfer Level; RTL): Синхронная параллельная модель электронной схемы, описывающая ее поведение посредством сигналов, обрабатываемых согласно комбинационной логике и передаваемых между регистрами по фронтам синхросигнала. Модель RTL, как правило, пишется на языке HDL или генерируется из исходного кода HDL.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

ASIC — специализированная интегральная схема;

CCF — отказ по общей причине;

CPLD — сложная программируемая логическая интегральная схема;

DRC — нормоконтроль;

ESL — уровень электронной системы;

FPGA — программируемая пользователем вентильная матрица;

HDL — язык описания аппаратуры;

HPD — HDL-программируемое устройство;

IP — интеллектуальная собственность ИС;

I&C — контроль и управление;

PAL — программируемая логическая матрица;

PDB — предварительно разработанный блок;

PDS — предварительно разработанное программное обеспечение;

PLD — программируемая логическая интегральная схема;

RAM — оперативное запоминающее устройство;

RTL — уровень регистровых передач;

SEU — отказ в результате единичного события;

SRAM[1)] — статическая оперативная память с произвольным доступом;

STA — статический временной анализ;

VHDL — язык описания аппаратуры интегральных схем;

V&V — верификация и валидация.

5 Общие требования к проектам HDL-программируемых устройств

5.1 Общие положения

В настоящем разделе сначала определено местоположение HPD в системе контроля и управления, описанной в МЭК 61513. Затем рассмотрен жизненный цикл разработки HPD, структурирующий проект HPD.

В настоящем стандарте установлены требования к проектам HPD, обеспечению качества и управлению конфигурацией, т. к. данные вопросы сходны с вопросами разработки программного обеспечения, требования устанавливают посредством ссылок на соответствующие разделы МЭК 60880, дополняемых специальными требованиями к HPD по мере необходимости.

В разделе 1 «Область применения» определено, что настоящий стандарт не устанавливает требования к разработке микроэлектронных технологий или заготовок интегральных схем. Следовательно, такие формулировки, как «разработка HPD», «жизненный цикл HPD», «конструкция HPD» или «верификация HPD», относятся к мероприятиям в рамках проекта по I&C, начиная с технологий или заготовок интегральных схем до разработки конкретных интегральных схем для применения в системе I&C.

5.2 Жизненный цикл

Процесс разработки систем I&C, важных для безопасности АС, рассмотрен в МЭК 61513, в котором вводится понятие «жизненный цикл системы». Это инструмент, посредством которого можно управлять процессом разработки и принятие которого дает обоснование правильной эксплуатации систем

[1)] Данное сокращение не используется в оригинальном тексте, сохранено для обеспечения идентичности перевода.

обеспечения безопасности. Жизненный цикл системы содержит и налагает требования на производство систем, но не диктует механизмы реализации проекта, которые будут использоваться для такого производства (см. рисунок 1).

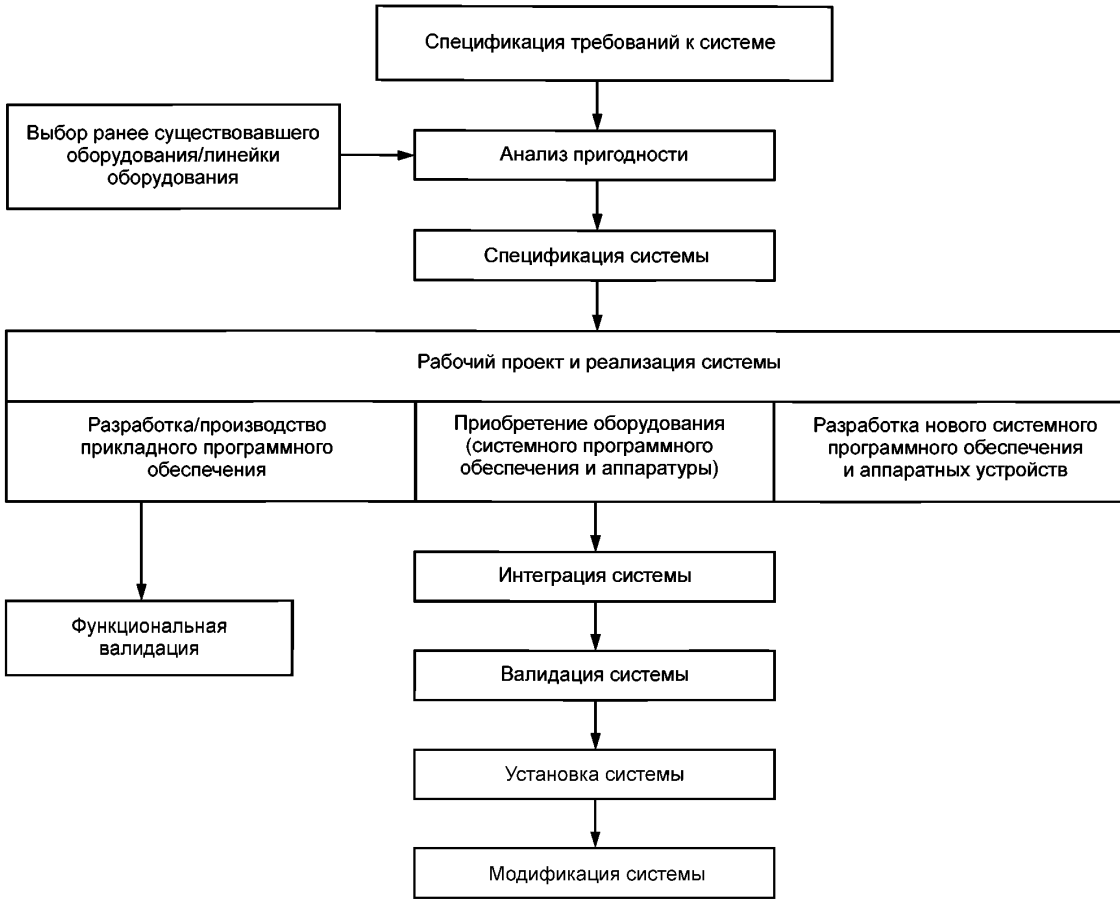

Рисунок 1 — Жизненный цикл системы (справочный, по МЭК 61513)

Жизненный цикл системы по МЭК 61513 дополнен в МЭК 60880 (для функций категории А), МЭК 62138 (для функций категории В и С) — для разработки программного обеспечения и в МЭК 60987 — для разработки аппаратуры компьютерных систем. Требования настоящего стандарта применяют к разработке HPD в системах класса 1, в дополнение к требованиям МЭК 60987.

Примечание — В случае противоречивых требований настоящий стандарт заменяет требования МЭК 60987 к HPD класса 1.

HPD разрабатывают посредством компьютерных инструментов, которые структурируют разработку согласно жизненному циклу, включающему в себя мероприятия по установлению требований, проектированию и реализации, интеграции и валидации наряду с мероприятиями верификации и тестирования.

Этапы проектирования и реализации системы по МЭК 61513, приведенные на рисунке 1 [в частности, «Приобретение оборудования» (системного программного обеспечения и аппаратуры) и «Разработка нового системного программного обеспечения и аппаратных функций»], являются основными этапами жизненного цикла системы по МЭК 61513. Этапы между спецификацией требований и валидацией для элементов системы, которые являются HPD, подробно проиллюстрированы на рисунке 2.

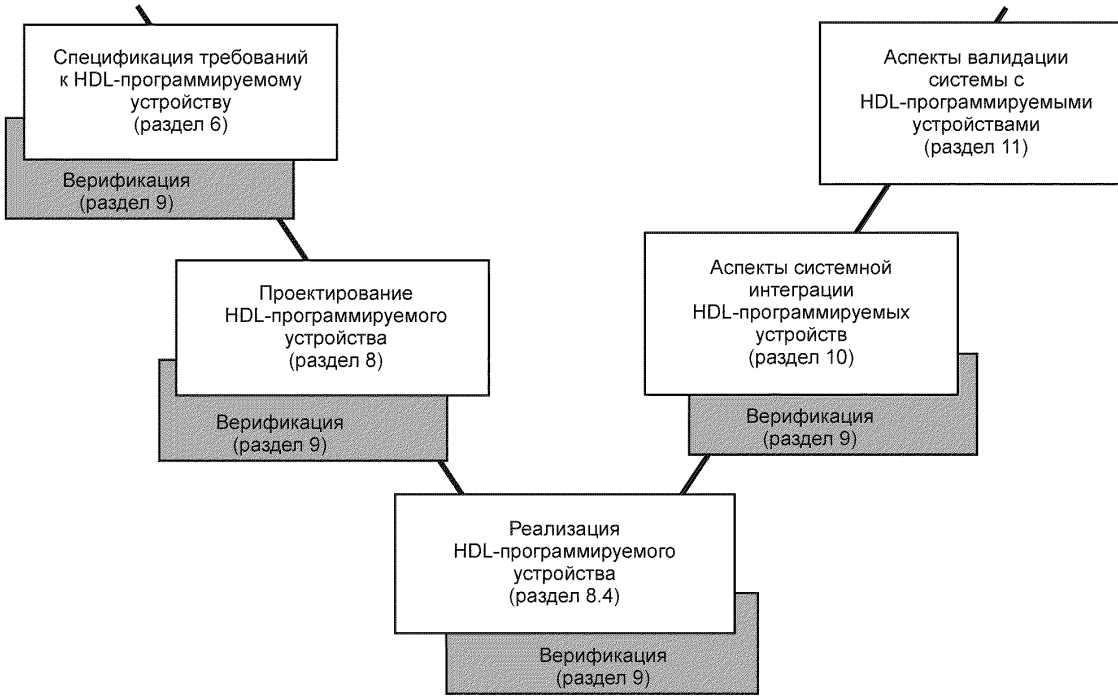

Рисунок 2 — Жизненный цикл разработки HPD

Как правило, проектировщики используют предварительно разработанные элементы, такие как программируемые заготовки интегральных схем или PDB, для построения интегральных схем, адаптированные под требования проекта. Мероприятия по выбору предварительно разработанных элементов приведены в разделе 7. Данные мероприятия можно проводить параллельно с первыми этапами жизненного цикла, представленного на рисунке 2, при условии, что все зависимости находятся под контролем и документально зафиксированы.

На рисунке 2 представлен жизненный цикл разработки HPD, который можно применять параллельно с разработкой других (программных или аппаратных) элементов системы, как показано на рисунке 1, но объединяемых на этапах интеграции и валидации жизненного цикла системы.

Предложенный подход к разработке основан на традиционной модели V-образной модели («цикла снижения — роста»), поскольку данный подход приведен в других стандартах и также рекомендуется в NS-G 1.3 МАГАТЭ. Данный подход позволяет вносить необходимые корректировки с учетом того, что некоторые этапы разработки могут быть выполнены автоматически инструментами и что разработка может носить итерационный характер.

Как правило, отсутствует явное разделение и четко определенная граница между интеграцией данного элемента и интеграцией на уровне системы. Таким образом, в настоящем стандарте интеграция HPD считается частью системной интеграции. Точно так же валидация HPD считается частью валидации системы.

В зависимости от функции, реализуемой HPD, рассматриваемая во время интеграции система или подсистема может варьироваться:

1) от системы I&C в случае, если HPD осуществляет логику функции безопасности;

2) до электронной платы или шкафа в случае, если HPD реализует функцию (внутреннюю по отношению к плате или шкафу), при этом с помощью надлежащего анализа было подтверждено, что она не может повлиять на выходные сигналы какой-либо функции безопасности на других уровнях системы.

Как правило, ситуация наиболее критична с точки зрения безопасности в том случае, если HPD непосредственно реализует логику функции безопасности.

Процесс разработки HPD включает в себя следующие мероприятия:

a) управление проектом (см. 5.3);

b) обеспечение качества и контроль качества (см. 5.4);

c) управление конфигурацией (см. 5.5);

d) верификация (см. раздел 9).

Существуют также мероприятия, касающиеся выбора инструментов для поддержки разработки (см. раздел 15), подготовки документации (см. приложение А) и модификации (см. раздел 12).

5.3 Управление проектом HDL-программируемого устройства

5.3.1 Общие положения

5.3.1.1 Каждое HPD необходимо разрабатывать в рамках специализированного проекта HPD.

5.3.1.2 Необходимо, чтобы проект HPD соответствовал требованиям МЭК 60880:2006 (подраздел 5.4) (заменяя термин «программное обеспечение» на термин «HPD»).

Примечание 1 — Типовой перечень документов, необходимых на протяжении жизненного цикла, приведен в приложении А.

Примечание 2 — Документально зарегистрированные входные данные, рассмотренные в МЭК 60880:2006 (пункт 5.4.6), включают в себя параметры для автоматизированных действий программных инструментов (например, оптимизировать синхронизацию, оптимизировать плотность и т. д.).

5.3.1.3 Процесс разработки может быть итерационным, следующий этап может начаться до завершения мероприятий предыдущего этапа. Однако этап необходимо завершать, только если предыдущие этапы выполнены и результаты данного этапа согласуются с входными данными, полученными от предыдущих мероприятий.

5.3.1.4 В этапы проекта HPD необходимо включить спецификацию требований, проектирование и реализацию HPD.

5.3.2 Дополнительные требования

5.3.2.1 Предварительно разработанные элементы, используемые в проекте, необходимо выбирать согласно требованиям раздела 7.

5.3.2.2 Необходимо установить критерии перехода от одного этапа к другому.

5.3.2.3 Необходимо обеспечить методологическое и техническое содержание критериев для завершения этапа, включая подробную информацию, вследствие чего их оценка требует всестороннего анализа результатов этапа.

5.3.2.4 В документацию, согласно требованиям МЭК 60880:2006 (пункт 5.4.11), необходимо включить описание функций, выполняемых HPD и его интерфейсом.

5.4 План обеспечения качества HDL-программируемого устройства

Необходимо наличие плана обеспечения качества HPD, соответствующего требованиям МЭК 60880:2006 (подраздел 5.5) (заменяя в требованиях термин «программное обеспечение» на термин «HPD»).

Примечание — В данном контексте «язык» означает «компьютерный язык».

5.5 Управление конфигурацией

5.5.1 Управление конфигурацией HPD необходимо выполнять согласно требованиям МЭК 60880:2006 (подраздел 5.6), заменяя в требованиях термин «программное обеспечение» на термин «HPD».

Примечание — Разделение, требуемое согласно МЭК 60880:2006 (подраздел 5.5) относится к документации и компьютерным файлам, используемым или полученным в проекте HPD.

5.5.2 Необходимо, чтобы при управлении конфигурацией фиксировались следующие элементы:

a) документация модулей (блоков), разработанных в рамках проекта, и PDB;

b) идентификационная маркировка интегральных схем;

c) компьютерные файлы, используемые для моделирования, верификации и производства;

d) параметры, используемые для автоматизированных действий инструментальных программ (см. раздел 15), таких как «оптимизировать синхронизацию, оптимизировать плотность», для действия «размещение и трассировка»;

e) идентификация версий всех инструментальных программ (см. раздел 15), включая любые примененные программные корректировки, а также библиотеки общего назначения и технологические библиотеки.

6 Спецификация требований к HDL-программируемому устройству

6.1 Общие положения

6.1.1 В спецификации требований необходимо документально зафиксировать требования к HPD, либо непосредственно в самой спецификации, либо ссылаясь на совокупность требований, установленных на уровне системы или подсистемы (например, реализуемое функциональное поведение).

6.1.2 Необходимо, чтобы спецификация требований была понятной для всех участников, включая инженеров по разработке аппаратуры и лиц, упомянутых в 6.6.

6.1.3 Необходимо, чтобы спецификация требований была однозначной, верифицируемой и достижимой, в том числе по временным аспектам.

6.1.4 В случае если HPD реализует функцию безопасности, необходимо, чтобы его спецификация требований следовала из требований системы I&C, осуществляющей данную функцию безопасности, и была частью спецификации подсистемы, которая использует HPD.

6.1.5 Необходимо, чтобы спецификация требований содержала описание того, что должно быть сделано, а не как оно должно быть сделано.

6.1.6 Для разработки спецификации требований необходимо определить и реализовать документально фиксируемый, формальный и подконтрольный процесс.

6.1.7 Спецификация требований должна позволять проверку соответствия спецификации требований системы I&C. Если HPD применяется подсистемой системы I&C, то должна быть возможна проверка соответствия спецификациям проекта системы.

6.1.8 Необходимо, чтобы спецификация требований рассматривала все рабочие состояния АС до уровня HPD для реализуемых функций.

6.1.9 Необходимо рассмотреть требования к интерфейсу с другими системами или элементами согласно МЭК 61513.

6.1.10 Необходимо документально зафиксировать требования к интерфейсу с другими системами или элементами.

6.1.11 В случае если данные требования не являются частью требований HPD, но следуют из проектных решений HPD, необходимо документально зафиксировать следующие требования к интерфейсу:

a) электрические и временные характеристики (например, входная нагрузка, установка и время удержания входных сигналов, рабочая частота, коэффициент разветвления по выходу, время распространения от любого входа к соответствующим выходам);

b) профили сопрягаемого сигнала и источников электропитания;

c) требования к рассеиванию мощности, рабочей температуре и охлаждению.

6.2 Функциональные аспекты спецификации требований

В настоящем подразделе приведено содержание спецификации требований, непосредственно связанных с функциональными потребностями. Подразделы 6.3 и 6.4 рассматривают дополнительные аспекты, подлежащие включению в спецификацию требований.

В спецификации требований необходимо указать:

a) функции, реализуемые HPD;

b) различные режимы HPD и соответствующие условия перехода, включая подачу электропитания и инициализацию;

c) интерфейсы HPD и взаимодействия с окружающей средой (операторами и другими элементами I&C), включая роли, протоколы, типы, форматы данных, нумерацию битов, диапазоны и ограничения входных и выходных сигналов;

d) параметры HPD, которые можно модифицировать вручную при эксплуатации, и их роли;

e) эксплуатационные характеристики HPD, в частности быстродействие;

f) информацию о том, что HPD не должно делать при необходимости;

g) предположения относительно окружающей HPD среды (например, электрические и временные характеристики входных и выходных сигналов, источников электропитания, заданные профили при подаче электропитания, охлаждении).

6.3 Детерминированное проектирование

В спецификации требований необходимо указать, что функция HPD детерминирована умышленно. Это означает, что любая данная входная последовательность, выполняющая электрическую и временную спецификацию, всегда производит одинаковые выходные сигналы.

Примечание — Современные FPGA и другие интегральные схемы, рассматриваемые в настоящем стандарте, могут содержать в себе аналоговые функциональные блоки (например, аналого-цифровой преобразователь), которые подвергаются электронным помехам, погрешностям оцифровки и т. д. Изменения в отклике названных аналоговых функциональных блоков по указанным причинам, так же как их воздействия на отклик HPD, не являются нарушениями в детерминированной конструкции.

6.4 Обнаружение отказов и устойчивость к неисправностям

Применяют требования МЭК 60987 (подразделы 5.3 и 5.4), рассматривающие надежность относительно случайных отказов и допустимых климатических условий. Сюда входят неисправности, обусловленные SEU нейтронного или альфа-излучения.

Защитный проект, как правило, основан на сочетании методик (например, резервирование, мажоритарная выборка, контроль по четности и контроль с использованием циклического избыточного кода, сторожевой таймер, контроль по диапазону и проверка правдоподобия).

6.4.1 В спецификации требований необходимо определить требования к защитному проектированию, чтобы рассмотреть обнаружение отказов и устойчивость к дефектам и ошибкам.

6.4.2 Преимущество мер защитного проектирования следует уравновесить их вынужденной дополнительной сложностью. Общая цель состоит в том, чтобы принять во внимание контролируемость HPD во время проектирования и реализации с помощью внутренних и внешних средств обнаружения для выявления неисправностей.

6.4.3 В спецификации требований необходимо привести положения по обнаружению нарушений функционирования HPD с учетом положений, уже принятых на уровне системы или подсистемы.

6.4.4 Эти положения могут потребовать от HPD дополнительных выходных сигналов либо для использования внешнего механизма, такого как сторожевой таймер, либо для достижения покрытия контроля, выполняемого внешним испытательным устройством.

6.4.5 Защитное проектирование должно обеспечивать обнаружение ошибочного поведения (такого, как повреждение данных, или отклонение от указанного алгоритма обработки, или отклонение от заданных рабочих состояний), ошибочной передачи данных между блоками обработки, непреднамеренного изменения данных конфигурации или памяти.

6.4.6 Защитное проектирование не должно оказывать неблагоприятного влияния на функции системы I&C и препятствовать тому, чтобы HPD соответствовало спецификации быстродействия.

6.4.7 В спецификации требований необходимо привести описание ожидаемого логического и временного поведения (такого, как выходные значения и выдаваемая конкретная информация) при обнаружении неисправности.

6.4.8 Необходимо, чтобы указанное поведение соответствовало поведению системы, требуемому спецификацией системы, и удовлетворяло требованиям проектирования системы в соответствии с МЭК 61513.

6.4.9 В спецификации требований необходимо указать и обосновать целевое покрытие обнаружения отказов, которое будет достигнуто с помощью защитного проектирования.

6.5 Определение требований с помощью инструментов проектирования на уровне электронных систем

6.5.1 Общие сведения

Настоящий стандарт не устанавливает конкретного метода для определения требований к HPD. В случае если их определяют с помощью инструментов проектирования электронных систем на системном уровне (ESL) (см. приложение В, пункт В.1), то к этим инструментам и их использованию применяют требования 6.5.2 и 6.5.3.

В случае ESL, т. к. язык спецификации требований может быть аналогичен языкам реализации, выполнение требований 6.1.5 может оказаться менее практичным [разделение между тем, что должно быть сделано (требование) и как это сделано (проектирование)]. Для выполнения данного требования могут потребоваться условия, например, комментарии, уточняющие входные, выходные сигналы и алгоритмы.

6.5.2 Требования в отношении формального подхода к инструментам, используемым на уровне ESL

6.5.2.1 В случае если требования к HPD определены с помощью инструмента ESL:

a) данный инструмент должен предложить формальный подход со строгой семантикой и ясностью (стандартизация структуры и представления, модульность, обоснованные комментарии);

b) необходимо, чтобы формальный подход, используемый в инструменте ESL, был понятен для всех участников;

c) если инструмент предлагает гибкие механизмы пересмотра определения функций и операторов, то фактические характеристики любого данного элемента должны быть ясны любому участнику, включая инженеров по разработке аппаратуры и прочий персонал, упомянутый в 6.6.

6.5.2.2 Языки, используемые на уровне ESL, должны позволять должным образом учесть архитектуру системы, например, позволить назначение функций элементам, и поддерживать любые отказоустойчивые особенности конструкции.

6.5.3 Интерфейс со средствами проектирования

Семантика языков, используемых для выражения спецификации требований на уровне ESL, может отличаться от семантики языков HDL, используемых при проектировании. Примеры того, где могут возникнуть расхождения, находятся в интерпретации параллелизма, управлении переполнением или кодировании типов и конечных автоматов:

a) если семантика языка, используемого для выражения спецификации требований на уровне ESL, отличается от семантики других используемых в проекте языков, то расхождения необходимо идентифицировать для каждого фигурирующего элемента спецификации требований;

b) каждое возникновение расхождения в спецификации требований необходимо документально зафиксировать. Примерный перечень расхождений между фигурирующими языками является полезной ссылкой, но недостаточен для разъяснения спецификации требований.

6.6 Анализ и обзор требований

6.6.1 Необходимо выполнить и документально зафиксировать критический анализ требований, чтобы найти потенциальные несогласованности, упущения и неоднозначности.

6.6.2 Данный анализ должен охватывать функциональные требования и все прочие типы требований, включая те, которые рассматривают нештатное поведение, например, неожиданные входные значения или последовательности.

6.6.3 Необходимо сделать критический обзор спецификации требований для проверки на полноту и согласованность.

6.6.4 Для функций обеспечения безопасности, реализованных в HPD, в критическом обзоре необходимо участие технологов и инженеров I&C, а также специалистов по подсистемам или элементам (включая программное обеспечение), сопрягаемым с HPD.

7 Процесс обоснования применения для программируемых интегральных схем, конфигурируемых блоков и предварительно разработанных блоков

7.1 Общие положения

При разработке HPD необходимо выбрать и оценить предварительно разработанные элементы, такие как заготовка интегральной схемы (включая конфигурируемые блоки) или PDB, включаемые в конечное HPD.

Поскольку предварительно разработанные объекты (или элементы) могут включать в себя функции, не требуемые для HPD, то рекомендуется разработать и контролировать реализацию специфических «правил использования» для ограничения их применения тем, что необходимо и безопасно.

7.2 Спецификация требований к элементам

7.2.1 Общие положения

Требования, предназначенные для предварительно разработанных объектов (или элементов), вытекают из начальных мероприятий проектирования HPD. Например, требования к HPD могут включать в себя специфичный полосовой фильтр, который проектировщик может реализовать с помощью PDB, выполняющего быстрое преобразование Фурье.

Таким образом, спецификация требований к элементу (здесь — для PDB быстрого преобразования Фурье, определенного такими характеристиками, как тип алгоритма, размер основания, метод прореживания, размер кремниевого кристалла и т. д.) отличается от спецификации требований к HPD (здесь — для полосового фильтра, определенного такими характеристиками, как угловые частоты, коэффициент усиления, угол наклона кривой и т. д.).

7.2.1.1 В спецификации требований к элементу необходимо документально зафиксировать требования, применимые к каждому предварительно разработанному элементу: заготовка интегральной схемы, микроэлектронные ресурсы (в виде конфигурируемых блоков), сопутствующие инструменты в соответствующих случаях или PDB.

7.2.1.2 В спецификации требований к элементу необходимо установить все требования, либо непосредственно в самой спецификации, либо посредством ссылки на наборы требований, установленные на уровне системы или подсистемы (например, реализуемое функциональное поведение).

7.2.1.3 Являясь основанием для выбора и применения предварительно разработанного элемента, спецификация требований к элементу должна быть понятной всем участникам, включая разработчиков аппаратных средств и программного обеспечения в соответствующих случаях, а также контролерам, рецензентам и представителям регулирующих организаций.

7.2.1.4 Необходимо, чтобы спецификация требований к элементу была однозначной, верифицируемой и достижимой, в том числе по временным аспектам.

7.2.1.5 Необходимо, чтобы спецификация требований к элементу позволяла продемонстрировать соответствие требованиям МЭК 61513 к системе I&C, использующей этот элемент.

7.2.2 Требования

В спецификации требований к элементу необходимо указать все характеристики, требуемые от предварительно разработанного элемента, в частности из перечня, приведенного в 6.2.

Примечание — Обобщенные названия характеристик (например, «функция») идентичны указанным в 6.2, но их содержание отличается, см. 7.2.

7.2.3 Анализ и обзор требований

7.2.3.1 Необходимо выполнить и документально зафиксировать критический анализ спецификации требований к элементу для того, чтобы найти потенциальные несогласованности, недостаточную полноту или неоднозначность.

7.2.3.2 Данный анализ должен охватывать функциональные требования и все прочие типы требований, включая те, которые рассматривают нештатное поведение, например неожиданные входные значения или последовательности.

7.2.3.3 Необходимо, чтобы спецификация требований к элементу была формально рассмотрена экспертами всех соответствующих предметных областей для проверки на полноту и согласованность.

7.3 Правила использования

7.3.1 В случае если предварительно разработанный элемент включает в себя функции или эксплуатационные режимы, реализация которых в HPD не требуется, то в правилах устанавливают запрет на использование таких функций и режимов.

Использование функций или режимов, требующихся для реализации HPD, может быть ограничено правилами в целях улучшения проектных параметров, таких как безопасность или контролепригодность.

7.3.2 Если установлены правила использования, то:

a) необходимо их документально зафиксировать;

b) план обеспечения качества должен гарантировать, что их выполнение проверяется в ходе реализации проекта.

7.4 Выбор

7.4.1 Общие положения

7.4.1.1 В документально фиксируемом анализе каждого предварительно разработанного элемента, применяемого в HPD, необходимо показать, что он удовлетворяет требованиям спецификации к данному элементу и, возможно, требованиям по его использованию и модификации (см. 7.6).

7.4.1.2 В документации потребителя по безопасности необходимо подробно изложить, как проектировщикам применять предварительно разработанный элемент согласно его спецификации и проектным характеристикам.

7.4.2 Обзор документации

Обзор документации является основным методом подтверждения того, что предварительно разработанный элемент соответствует спецификации требований к элементу.

7.4.2.1 Данный обзор основан на документации предварительно разработанного элемента, включая документацию о его проекте и верификации.

7.4.2.2 Необходимо, чтобы документация содержала подробную информацию, которая позволит подтвердить соответствие функциональных, электрических и временных требований к предварительно разработанному элементу.

7.4.2.3 Во время проведения анализа документации необходимо удостовериться, что любые функции и режимы предварительно разработанного элемента, не используемые в HPD, не препятствуют используемым функциям и режимам.

7.4.3 Обзор опыта эксплуатации

Для компенсации некоторых ограниченных недочетов документации относительно надежности или конструкции предварительно разработанного элемента можно использовать опыт его эксплуатации.

Если используют опыт эксплуатации, то:

a) во время проведения анализа опыта эксплуатации необходимо подтвердить, что:

1) опыт соответствует требованиям надежности;

2) данный опыт накоплен в эксплуатационных условиях, эквивалентных условиям, в которых будет применяться предварительно разработанный элемент;

3) фактическое применение предварительно разработанного элемента прослеживается на уровне деталей, обычно требуемых настоящим стандартом для документации;

b) средства и процедуры, применяемые для накопления опыта эксплуатации, должны гарантировать, что любой отказ предварительно разработанного элемента, возникавший в анализируемом периоде эксплуатации, зарегистрирован настолько подробно, что проведение технического анализа позволяет идентифицировать причину данного отказа в максимально возможной степени;

c) посредством анализа отказов, зарегистрированных во время эксплуатации, необходимо удостовериться, что они не влияют на функции или безопасность HPD;

d) опыт эксплуатации и, при необходимости, дополнительные испытания должны подтвердить, что предварительно разработанный элемент соответствует требованиям, предъявляемым к нему;

e) в документально фиксируемом техническом анализе необходимо обосновать, что все взаимодействия предварительно разработанного элемента с окружающей средой включены в число взаимодействий, охваченных опытом эксплуатации;

f) необходимо, чтобы проанализированный опыт эксплуатации соответствовал точно определенным версиям предварительно разработанного элемента, а в случае, если этот элемент характерен для оборудования, то оборудования, в котором он функционирует;

g) в опыте эксплуатации следует рассмотреть конкретную версию предварительно разработанного элемента или его части, используемой в HPD, или проанализировать различия между версиями для подтверждения соответствия опыта эксплуатации намеченной версии.

7.4.4 Специфические требования в отношении заготовок интегральных схем

7.4.4.1 Необходимо рассмотреть следующие аспекты:

a) анализ адекватности программных механизмов и схемотехники;

b) демонстрация того, что процесс программирования безошибочен или что любой отказ в этом процессе будет обнаружен и должным образом урегулирован;

c) демонстрация того, что интегральная схема сохраняет свою программированную конфигурацию на протяжении адекватного интервала времени;

d) анализ потенциала возникновения отказов, обусловленных дополнительными внутренними и внешними механизмами или переходными процессами электропитания, и обоснование согласно требованиям надежности.

7.4.4.2 Во время проведения подробного анализа необходимо подтвердить, что:

a) интегральная схема будет соответствовать спецификации требований к элементу;

b) сопутствующие инструменты:

- соответствуют разделу 15;
- позволяют проведение всех верификаций, требуемых разделами 8 и 9 (таких, как STA).

7.4.4.3 Данные, необходимые для вычисления интенсивности отказов (т. е. случайных физических отказов), должны быть доступны и основаны на достаточном опыте эксплуатации.

7.4.4.4 Необходимо, чтобы проектировщики, конструирующие или реализующие HPD, обладали адекватным знанием:

a) о заготовке интегральной схемы, включая особенности программирования, режимы конфигурации и испытания, протоколы, контакты и регистры, любую электрическую или логическую специфику;

b) о сопутствующих инструментах, конфигурируемых блоках и PDB. В частности, они должны быть в состоянии предсказать, понять и (при необходимости) управлять выбором, сделанным инструментами во время синтеза, размещения и трассировки.

7.5 Подтверждение обоснования применения

7.5.1 Во время проведения формальной экспертизы необходимо изучить результаты анализа предварительно разработанного элемента, включая правила использования и меры, принятые в целях гарантии соответствия техническим условиям каждой физической части, используемой в производстве, для того чтобы решить, принимается ли предварительно разработанный элемент для использования в HPD.

7.5.2 В случае если предварительно разработанный элемент принимают для применения, то любые учтенные при проведении анализа меры и правила применения должны распространяться на весь жизненный цикл HPD.

7.5.3 В комиссию необходимо включить специалистов, обладающих навыками в соответствующих областях (например, аппаратная технология, программное обеспечение), и инженеров из коллективов, ответственных за элементы, сопрягаемые с предварительно разработанным элементом.

7.6 Модификация для обоснования применения

7.6.1 В случае если для обоснования применения предварительно разработанного элемента необходимы модификации, то их необходимо определить, разработать, реализовать и проверить перед выполнением экспертизы.

7.6.2 Данные модификации необходимо выполнить и документально зафиксировать в соответствии с требованиями настоящего стандарта к структуре проекта и управлению, качеству, спецификации требований, проектированию, реализации и верификации.

7.7 Модификация после обоснования применения

Мероприятия по обоснованию применения, включая экспертизу, необходимо выполнять снова после любой модификации предварительно разработанного элемента, включая его конструкцию или микроэлектронные аспекты.

7.8 Документация для обоснования применения

Документация для обоснования применения предварительно разработанного элемента должна находиться под управлением конфигурацией.

7.8.1 В документацию необходимо включить или сослаться на:

a) спецификацию требований к HPD;

b) документы, разработанные или примененные при анализе предварительно разработанного элемента;

c) документы, разработанные при модификации предварительно разработанного элемента;

d) акт.

В документацию следует включить информацию, необходимую для правильного применения предварительно разработанного элемента с учетом ограничений из его начальной спецификации, правил использования и модификаций.

8 Проектирование и реализация HDL-программируемого устройства

8.1 Общие положения

Настоящий раздел устанавливает требования и рекомендации, основанные на надлежащей практике проектирования и реализации, направленные на соответствие адекватным функциям обеспечения безопасности, таким как максимальная безотказность и восприимчивость к верификации.

8.1.1 В процессе разработки необходимо определить этап проектирования и этап реализации.

8.2 Языки описания аппаратуры и сопутствующие инструменты

Несмотря на то, что может не требоваться применение конкретных языков и инструментов в качестве общих основных правил применения языков и инструментов, используемых при проектировании и реализации HPD для систем класса 1, можно рассмотреть следующее.

8.2.1 При проектировании и реализации используют HDL и инструменты для моделирования, синтеза, размещения и трассировки.

Примечание — При должном выборе и использовании данные инструменты улучшают существенно важные аспекты, такие как понятность описаний, управление электрическими и временными ограничениями, верификация, адекватность критериев покрытия и документация.

8.2.2 В случае если требование 8.2.1 не выполняется, необходимо предоставить всю документацию, провести анализ или верификацию, требуемые настоящим стандартом.

8.2.3 Необходимо, чтобы применяемый язык:

a) следовал строгим (или четко определенным) семантическим и синтаксическим правилам;

b) обладал полно и четко определенным и документально зафиксированным синтаксисом;

c) соответствовал признанному стандарту (например, IEEE 1076 для VHDL или IEEE 1364 для Verilog).

8.2.4 В надлежащих случаях использование языка ограничивают «безопасным» подмножеством, например ограничивают инструментарием, необходимым для реализации требуемых функций и синтезируемым с помощью стандартизированных библиотек (например, избегают использования начальных значений, явных задержек или деления).

8.2.5 Необходимо, чтобы используемый симулятор выдавал результаты, строго согласующиеся с документально зафиксированной семантикой языка.

Симулятор должен соответствовать признанному стандарту (например, IEEE 1076 для VHDL или IEEE 1364 для Verilog).

8.2.6 За исключением случаев, приведенных в 8.2.7, для анализа, моделирования, синтеза, размещения и трассировки необходимо использовать только те инструменты, которые соответствуют требованиям раздела 15. Потребителям *допускается* не проводить повторно испытания инструментов, если данные испытания уже были проведены и документально зафиксированы поставщиком.

8.2.7 В случае если применяют инструмент, не соответствующий в полном объеме требованиям раздела 15, то достоверность результатов, полученных данным инструментом, необходимо подтвердить с помощью дополнительной верификации результатов (например, перечень связей, получаемый инструментом синтеза). Формальные инструменты контроля эквивалентности являются важным средством получения безошибочной конструкции.

8.3 Проектирование

8.3.1 Общие положения

Начиная со спецификации требований к HPD, при проектировании изначально стремятся определить главные направления выбора, такие как разложение на модули (зависящие от типа приложения или предварительно разработанные), эксплуатация защитного проекта, а также идентификация необходимых микроэлектронных технологий (включая их конфигурируемые блоки) и PDB. Затем строят описание RTL с помощью HDL. Для создания ясной и верифицируемой конструкции установлены следующие требования.

8.3.1.1 На этапе проектирования необходимо получить:

a) формализованное описание HPD, например RTL;

b) сопутствующую документацию.

8.3.1.2 Необходимо разработать линии связи в соответствии с требованиями по передаче данных, установленными в МЭК 61513 (подпункт 5.4.2.4).

8.3.1.3 Конструкция должна позволять проведение простой верификации.

8.3.1.4 Несоблюдение правил проектирования необходимо обосновать.

8.3.2 Защитное проектирование

8.3.2.1 В случае если выбранный конфигурируемый блок или PDB (см. раздел 7) является ядром процессора, то он должен соответствовать требованиям МЭК 60880 к самоконтролю.

8.3.2.2 В конструкции необходимо учитывать меры, избранные в спецификации требований для обнаружения неисправностей и выработки соответствующей информации в HPD.

8.3.2.3 Необходимо, чтобы при обнаружении отказа поведение HPD соответствовало установленным требованиям.

8.3.3 Структура

8.3.3.1 Нисходящий подход к проектированию предпочтителен восходящему подходу.

Примечание — Элементы библиотеки представляют собой конечные цели проектирования. Таким образом, использование библиотек, удовлетворяющих требованиям разделов 7 и 15, соответствует нисходящему подходу и рекомендуется к применению.

8.3.3.2 Структура конструкции основана на разложении на модули. Соответствующие модули могут содержаться в библиотеке.

8.3.3.3 Унифицированные модули содержатся в библиотеках.

8.3.3.4 Структура конструкции должна быть проста и понятна как в целом, так и в деталях.

8.3.3.5 Концептуальную модель архитектуры генерируют в начале проекта.

8.3.4 Язык и правила кодирования

8.3.4.1 Для того чтобы обеспечить устойчивую и надежную конструкцию, используют отработанную методологию проектирования и общую надлежащую практику.

8.3.4.2 Для того чтобы сделать конструкцию более понятной и уменьшить потенциал для различий между моделируемым и синтезируемым поведением:

a) необходимо по требованию плана обеспечения качества установить ряд строгих правил проектирования, отражающих новейшие знания с точки зрения конструкционной безопасности и надежности;

b) соответствие указанным правилам проектирования необходимо внедрять адекватными средствами (например, экспертиза, оснащение и т. д.).

8.3.4.3 Приведенный в настоящем пункте перечень рекомендуемых положений и методик проектирования не является всеобъемлющим и может быть актуализирован с изменением технологий. Тем не менее любое несоблюдение приведенных ниже правил необходимо обосновывать и учитывать при анализе отказа:

a) при проектировании HPD используют только синтезируемые функции языка. Среда испытания и моделирования (см. 9.5) может использовать все языковые функции. Любые конфигурируемые блоки (см. 3.9), которые уже синтезированы и разведены в предварительно разработанной интегральной схеме, можно инстанцировать как есть, если они соответствуют требованиям раздела 7;

b) в соответствующих случаях используют специализированные ресурсы или конструктивные особенности (например, предопределенные распределения и схемы формирования тактовых сигналов, шины электропитания, деревья сброса и т. д.);

c) правила кодирования охватывают все аспекты, в частности наименование модулей и сигналов, использование функций структурирования (таких, как пакеты, функции, процедуры, проектные библиотеки, конкретизация объекта), организация вычислений по критическим путям, организация процессов, рекомендуемые конструкции, запрещенные конструкции;

d) в описании проекта следует запретить функции, использующие побочные эффекты. (Обоснование: данная функция может возвращать различные значения, если ее вызывать несколько раз с одинаковыми параметрами. Указанную функцию трудно испытывать и верифицировать, т. к. она нарушает фундаментальное понятие функции и фактически — детерминированное поведение программы.)

Примечание 1 — Указанные функции могут также обладать такими побочными эффектами, как модификация объектов из их области действия;

e) следует запретить конструкции, которые могут вызвать различия между моделируемым и синтезируемым поведением. В зависимости от используемого языка примерами таких конструкций могут служить неполные или противоречивые назначения, использование безразличного символа в сравне-

ниях, сравнения («больше» или «меньше») с включением перечисляемых типов. (Обоснование: моделирование является важным методом верификации. Если моделируемое и синтезируемое поведения различаются, то цепь верификации разрывается);

f) сигналы и переменные следует инициализировать не при их декларации в описании RTL, а с помощью некоего явного механизма, такого как сброс. (Обоснование: инициализация в HDL может привести к различиям между моделируемым и синтезируемым поведением);

g) следует запретить использование явных задержек в проектном описании, поскольку такие задержки приводят к различиям между моделируемым и синтезируемым поведением;

Примечание 2 — Данное правило не запрещает существование задержек на уровне системы или в требованиях к HPD. Это означает, что такие задержки нельзя реализовать командой «delay» («задержка») или «after» («после») в HDL, но можно, например, с помощью счетчиков или сдвиговых регистров.

h) в проектном описании следует запретить создание задержек посредством комбинационных схем совпадений или посредством зависимости от задержек распространения по проводам. Если такое проектирование неизбежно, то необходимо выполнить STA, чтобы оправдать использование такой конструкции. (Обоснование: указанные задержки не устойчивы по параметрам, таким как температура, напряжение, или от одной части до другой, или от одной зоны кристалла интегральной схемы до другой);

i) типы сигналов интерфейса HPD следует определить ясным и однозначным образом, предпочтительно стандартизированным, независимо от инструментов или микроэлектронных технологий;

j) определения уровня HDL не должны допускать различные интерпретации во избежание вариаций при компиляции в различных условиях. Например, входные/выходные сигналы HPD явно назначают на известные контактные выводы схемы.

Примечание 3 — Требования настоящего подраздела не применимы к проектированию элементов библиотеки, которые строят для реализации в различных местоположениях будущих конструкций с различными распределениями ввода/вывода.

Примечание 4 — Для разработки кода HDL, который можно передавать между различными технологиями, необходимо определить назначение контактных выводов в файле ограничений, а не в коде HDL. Помочь в этом могут языковые функции, такие как шаблоны в VHDL-2008.

8.3.5 Синхронная и асинхронная конструкция

Синхронность конструкции состоит в принудительном выполнении изменения состояния внутренних регистров и выходных сигналов одновременно только в задаваемые генератором синхроимпульсов моменты времени, что благоприятствует созданию модульной и понятной конструкции, минимизирует потенциал для некорректного поведения из-за сбоев и способствует наилучшему использованию инструментов синтеза и верификации.

8.3.5.1 Для того чтобы упростить устойчивые, робастные и ясно структурированные конструкции, необходимо:

a) использовать строго синхронную архитектуру;

b) обосновать факты несоблюдения.

8.3.5.2 Необходимо, чтобы спроектированная конструкция гарантировала синхронизацию сигналов в асинхронных интерфейсах.

8.3.5.3 При использовании асинхронной архитектуры при проведении документально зафиксированного анализа всех межсоединений необходимо удостовериться в соответствии выходных сигналов спецификации требований (см. раздел 6) и отсутствии неблагоприятных сбоев или метастабильности.

8.3.5.4 Поведение HPD не должно быть подвержено изменениям из-за фактических значений внутренних временных задержек распространения сигнала по проводам и через шлюзы.

8.3.6 Управление режимом электропитания

8.3.6.1 Необходимо, чтобы внутренние электрические и временные характеристики заготовки интегральной схемы во время включения электропитания/запуска, выключения электропитания и внезапной потери электропитания были известны и учтены в ходе проектирования.

8.3.6.2 Информацию о поведении каждого контактного штыря (например, входного или выходного типа, импеданс) при включении электропитания/запуске, выключении электропитания и внезапной потере электропитания необходимо документально зафиксировать.

8.3.6.3 Использование HPD на основе программируемой технологии не должно полагаться на допущение того, что они ведут себя в соответствии со своим запрограммированным режимом (относительно, например, функций, направления и импеданса каждого контактного штыря) при включении

электропитания/запуске, выключении электропитания и внезапной потере электропитания, даже в случае одноразовых запрограммированных устройств.

8.3.6.4 Соединение входных контактных штырей с источником напряжения или с землей выполняют согласно полученным от поставщика указаниям по применению, чтобы избежать потенциальных токовых пиков при включении электропитания/запуске, выключении электропитания и внезапной потере электропитания.

8.3.6.5 В случае если распределение электропитания не установлено поставщиком элементов, необходимо его особо предусмотреть при проектировании, чтобы избежать недетерминированных отказов из-за таких проблем, как изменения напряжения в переходном режиме, обусловленные токовыми пиками на фронтах синхроимпульса.

8.3.7 Инициализация

8.3.7.1 Необходимо, чтобы у конструкции имелся входной сигнал, приводящий все выходные сигналы, регистры и конечные автоматы в известное и документально зафиксированное состояние.

8.3.7.2 Необходимо, чтобы сигнал инициализации, который не всегда имеет чисто цифровую природу, соответствовал требованиям заготовки интегральной схемы, таким как время нарастания, время спада импульса или монотонность.

8.3.7.3 Необходимо, чтобы подтверждение данного сигнала оказывало намеченное влияние, даже когда никаких действий синхронизации не происходит.

8.3.7.4 Отмену подтверждения этого сигнала необходимо выполнять таким образом, чтобы поддерживать все выходные сигналы, регистры и конечные автоматы в их начальном известном состоянии до начала синхронизации.

8.3.8 Нефункциональные конфигурации

8.3.8.1 Необходимо проанализировать и сконфигурировать специальные контактные штыри и регистры, заставляющие HPD переключаться на специальные конфигурации (такие, как испытание, диагностика, отладка или программирование) и которые не определены спецификацией требований HPD, чтобы исключить любое неблагоприятное воздействие на его функции.

8.3.8.2 Проектировщики должны быть ознакомлены с документацией поставщика интегральных схем, чтобы знать характеристики, задаваемые инструментами неиспользуемым контактным штырям (входные, выходные, высокого импеданса и т. д.).

8.3.8.3 Необходимо документально зафиксировать управление контактными штырями и регистрами конфигурации HPD.

8.3.9 Контролепригодность

8.3.9.1 Необходимо, чтобы каждая функция, реализованная в HPD, была контролепригодной (обнаружение отказов) с помощью таких средств, как самопроверка, периодические испытания или поддающийся измерению вклад в высокоуровневую функцию, которая сама передается на самопроверки или периодические испытания.

8.3.9.2 При использовании устройств самопроверки необходимо проверить их способность выполнять свою функцию.

8.3.9.3 Необходимо определить фактическое покрытие обнаружения отказов (см. 6.4.9) и периодических испытаний и обеспечить его соответствие спецификации требований HPD.

8.3.9.4 Необходимо минимизировать последствия отказов, например, путем обнаружения таких состояний, которые обычно недостижимы, и осуществления в таких случаях предопределенного действия.

8.3.10 Проектная документация

8.3.10.1 Окончание этапа проектирования необходимо обозначить подготовкой соответствующей документации.

8.3.10.2 В документации необходимо описать и обосновать адекватность проектных решений при выполнении спецификации требований HPD.

8.3.10.3 Проектная документация должна быть всесторонней, чтобы реализация могла идти без дальнейших разъяснений.

8.3.10.4 В документации необходимо описать проектные решения, такие как:

a) организация в модулях, а также их интерфейсы и взаимосвязи;

b) потоки управления и тракты передачи данных;

c) протоколы и алгоритмы;

d) типы, форматы и логические обозначения сигналов;

e) нумерация шин, карта распределения памяти;

f) определения конечных автоматов, кодирование и инициализации;

g) инициализирующее значение всех регистров;

h) схема испытания.

8.3.10.5 В проектной документации необходимо определить вариант, фактически используемый для каждого экземпляра каждого элемента библиотеки, чтобы избежать неоднозначностей в том случае, если существуют варианты с различными быстродействиями или электрическими характеристиками.

8.3.10.6 В проектную документацию следует включить все параметры, необходимые для однозначного конфигурирования и использования всех конфигурируемых блоков и PDB.

8.3.10.7 В проектную документацию необходимо включить расчетные параметры синхронизации и электрические характеристики.

8.4 Реализация

8.4.1 Общие положения

Начиная с описания RTL реализация синтезирует описание на уровне логических сигналов (перечень связей) HPD. Затем выполняют размещение и трассировку, получая физическое описание, необходимое для изготовления HPD, такое как программирующий файл или «битовый поток».

8.4.2 Продукты

8.4.2.1 При реализации необходимо систематизировать всю информацию, необходимую для изготовления HPD и проверки того, что каждая изготовленная часть соответствует проекту.

8.4.2.2 При реализации необходимо подготовить информацию о синхронизации в дополнение к описанию RTL («обратное аннотирование»), чтобы точно смоделировать временно́е поведение с учетом всех задержек, связанных со схемами совпадений и проводами.

8.4.2.3 Необходимо, чтобы описание с обратным аннотированием было пригодным для испытательного стенда (см. 9.5) и, при необходимости, для высокоуровневых инструментов, таких как моделирование на уровне плат.

8.4.3 Файлы параметров и ограничений

Проектировщик направляет операции синтеза, размещения и трассировки с помощью параметров и директив, которые конкретизируют ограничения, такие как необходимая рабочая частота, соотношения синхронизации между сигналами или коэффициент разветвления по выходу. Для выполнения этих ограничений (получаемых инструментами в «файлах ограничений») инструменты могут модифицировать размещение, чтобы отдать предпочтение данному тракту распространения сигнала за счет других, дублировать одну логическую схему для снижения нагрузки на каждый экземпляр и таким образом увеличить их быстродействие и т. д.

Погрешности или упущения в параметрах и файлах ограничений могут привести к трудно диагностируемым недетерминированным отказам, которые часто нельзя обнаружить во время моделирования и которые чувствительны к нормальным вариациям технологического процесса в микроэлектронике.

8.4.3.1 Необходимо, чтобы файлы параметров и ограничений были построены согласно подконтрольному процессу.

8.4.3.2 Необходимо, чтобы полноту и правильность файлов параметров и ограничений проверила группа верификации (см. раздел 9).

8.4.3.3 Файлы параметров и ограничений необходимо документально зафиксировать и поместить под управление конфигурацией.

8.4.4 Пост-трассировочный анализ

8.4.4.1 При проведении пост-трассировочного анализа необходимо подтвердить соответствие проекта и реализации технологическим нормам, установленным поставщиком инструментов проектирования, и используемой микроэлектронной технологии.

8.4.4.2 Необходимо, чтобы пост-трассировочный анализ или моделирование (с учетом информации о пост-трассировочной синхронизации или обратного аннотирования) подтвердили пошаговую эквивалентность пост-трассировочного описания описанию RTL для самых быстрых и самых медленных случаев, включая инициализацию, например, с помощью двух следующих этапов:

a) подтверждение того, что описание после синтеза пошагово эквивалентно описанию RTL;

b) подтверждение того, что описание после трассировки соответствует ограничениям синхронизации.

8.4.4.3 При моделировании после трассировки допускается использовать подмножество случаев стендовых испытаний, применяемых в моделировании RTL (см. 9.5). Необходимо обосновать, что данное подмножество подтверждает эквивалентность. Альтернативный или дополнительный метод к моделированию после трассировки должен использовать инструмент, который проверит, что RTL и физический уровень описания математически эквивалентны. Если принят данный подход, необходимо перед его применением оценить качество и пригодность используемого для выполнения указанной проверки инструмента (см. раздел 15).

8.4.4.4 Необходимо проанализировать синхронизацию после трассировки.

8.4.4.5 Охват каждой функции самоконтролем необходимо проанализировать относительно требуемой цели (см. 6.4.9), учитывая возможное влияние инструментов на фактическую топологию.

8.4.4.6 Необходимо, чтобы данный анализ был достаточно подробным и зафиксирован документально, что позволит провести дальнейшую техническую оценку лицами, не занятыми в проектировании и реализации.

8.4.4.7 Некоторые виды данного анализа можно выполнить произвольно или автоматически с помощью инструментов. В таком случае не требуется выполнять заново, однако:

a) необходимо подтвердить, что виды анализа, выполняемого инструментами, обладают адекватным покрытием и правильностью;

b) отчеты об анализе (включая установку и результаты), получаемые с помощью инструментов, необходимо включить в документацию.

8.4.4.8 Если при анализе находят несоответствия, которые считают приемлемыми, то:

a) данную приемлемость необходимо обосновать и документально зафиксировать;

b) все затрагиваемые документы необходимо соответственно модифицировать;

c) необходимо, чтобы план обеспечения качества гарантировал, что любое влияние на другие системы или элементы документально фиксируют и соответственно учитывают лица, ответственные за затрагиваемые системы и элементы.

8.4.5 Избыточность, вводимая или удаляемая посредством инструментов

8.4.5.1 Необходимо проанализировать репликацию логических элементов, выполняемую инструментами для соблюдения соответствия ограничениям синхронизации или технологии.

8.4.5.2 Необходимо подтвердить, что дополнительные состояния, введенные данными репликациями, приемлемы относительно функциональных требований и норм техники безопасности. Признано, что репликация логических элементов выполняется многими инструментами синтеза, но, как правило, ею можно адекватно управлять непосредственно в самом инструменте. Однако требуется осторожность, т. к. репликация логических элементов может вызвать проблемы в том случае, если такая же формальная проверка эквивалентности используется для обоснования RTL и реализации логического элемента.

8.4.5.3 Поскольку репликация вводит новые состояния, их необходимо проанализировать и показать, что безопасное поведение конструкции не будет затронуто.

8.4.5.4 С другой стороны, необходимо подтвердить, что выполняемая инструментами логическая оптимизация не устранила механизмы обнаружения неисправностей и допуска, такие как резервирование или обработка случаев, в норме недостижимых.

8.4.6 Конечные автоматы

8.4.6.1 Необходимо проанализировать робастность окончательной реализации конечных автоматов.

8.4.6.2 В частности, у конечных автоматов не должно быть тупиковых состояний, кроме тех, которые могут быть определены в спецификации требований к HPD.

Примечание — Тупиковое состояние — это состояние, из которого конечный автомат не может достигнуть никакого другого состояния.

8.4.6.3 При анализе отказов необходимо учитывать потенциальные дополнительные состояния, введенные некоторыми методами кодирования (например, «прямое кодирование»).

Примечание — «Прямое кодирование» использует один триггер на представляемое состояние. Каждое конкретное состояние представлено одним конкретным триггером, установленным в состояние «истина», а все прочие установлены в «ложь». Таким образом, действительны только комбинации ровно с одним триггером, установленным в состояние «истина». В случае отказа несколько триггеров могут одновременно оказаться в состоянии «истина», что будет соответствовать дополнительным, неопределенным состояниям.

8.4.7 Статический временной анализ (STA)

8.4.7.1 Необходимо выполнить и документально зафиксировать STA для худших и лучших случаев для расчета запаса, с учетом информации о синхронизации, предоставленной технологическими библиотеками и всеми сопутствующими инструментами проектирования и реализации.

8.4.7.2 Если тракты исключены из STA (т. к. рассматриваются как «вспомогательные тракты») или объявлены как полицикличные тракты, то это решение необходимо обосновать и документально зафиксировать.

8.4.7.3 Необходимо, чтобы STA продемонстрировал, что частота каждого синхронизированного блока совместима со всеми неисключенными трактами (см. 8.4.7.2) с достаточным запасом в пределах заданной изменчивости микроэлектронной технологии.

8.4.7.4 Необходимо проанализировать и документально зафиксировать влияние расфазировки тактовых сигналов на критические структуры, например сдвиговые регистры.

Примечание — Расфазировка тактовых сигналов — это отрезок времени между поступлениями тактового сигнала в различных местоположениях.

8.4.8 Документация по реализации

Окончание этапа реализации необходимо обозначить подготовкой соответствующей документации, включая:

a) описание на уровне логических элементов HPD, годного к применению на том же испытательном стенде, который применяется на уровне RTL;

b) специальное техническое описание (например, «программирующий файл»), необходимое для программирования HPD и проверки каждой части (см. 13.2);

c) обратные аннотации, которые учитывают все задержки, связанные с логическими элементами и проводами;

d) синхронизации (такие, как частота, время установки и удержания, время нарастания и спада, время распространения) и электрические характеристики (такие, как уровни напряжения, входные токи, коэффициент разветвления по выходу, импедансы и потребление энергии), прогнозируемые инструментами, если они не определены в спецификации.

8.4.8.1 В документации по реализации необходимо:

a) дать доступ (включением или ссылкой) к реализации каждого блока, части блока или модуля;

b) привести сделанный выбор, в частности, в отношении контролепригодности, распределения тактовых сигналов и электропитания, сброса и реализации критических путей.

8.4.8.2 В документации по реализации необходимо привести и обосновать:

a) ограничения и параметры, передаваемые инструментам;

b) анализ, выполненный в целях гарантии соответствия HPD его спецификации требований, и любые обнаруженные различия;

c) любые итерации, выполненные при проектировании и реализации;

d) любое резервирование, введенное или удаленное во время реализации.

8.4.8.3 Необходимо, чтобы документация была достаточно подробной для того, чтобы инженер, не занятый в проекте, мог применять инструменты синтеза, размещения и трассировки и получать такие же результаты (выходные сигналы HPD и верификации), а также проверить полноту и правильность пост-трассировочного анализа.

8.4.8.4 В документации необходимо привести сведения об испытаниях, которые будут периодически проводиться при эксплуатации, с должной осторожностью в отношении структурных изменений, введенных инструментами.

8.4.8.5 В случае если перед началом производства требуется обязательство поставщика интегральных схем по проектированию или реализации, данное обязательство необходимо включить в документацию.

8.5 Инструменты системного уровня и автоматизированного кода

Требования различных элементов системы можно определить с помощью инструментов ESL, которые обеспечивают текстовое или графическое описание.

В настоящем подразделе приведено руководство, применимое в случаях, если описание ESL требований к HPD используют автоматизированным способом, чтобы частично или полностью сгенерировать конструкцию HPD. Указанную генерацию иногда называют «высокоуровневым синтезом».

8.5.1 Если спецификацию требований, написанную на языке ESL, применяют для автоматической генерации описания RTL HPD или его части:

a) сгенерированное описание следует составлять просто и избегать ненужной сложности;

b) данное описание должно позволять легко понимать поведение устройства, чтобы проектировщики аппаратуры могли быстро идентифицировать ошибки и неоднозначности.

8.5.2 Язык ESL и сопутствующие инструменты, в частности, используемые для генерации кода и анализа, соответствуют требованиям 8.2.

8.5.3 Если требование 8.5.2 не выполнено:

a) необходимо перевести описание ESL HPD в описание HDL, согласующееся с требованиями 8.2, которое будет основой следующих мероприятий по проектированию, реализации и верификации;

b) необходимо, чтобы указанные следующие мероприятия соответствовали требованиям настоящего стандарта.

8.5.4 Необходимо идентифицировать и обосновать любое несоответствие сгенерированных описаний (таких, как RTL, синтезируемый, трассированный) требованиям к проектированию и реализации (см. 8.3 и 8.4).

8.5.5 Если некоторые виды анализа, верификаций и обзоров, определенные настоящим стандартом в разделах 8, 9 и 10, не будут выполнены, то необходимо формально доказать, что продукты, которые не были проанализированы, верифицированы или рассмотрены, заведомо правильные.

8.5.6 Сгенерированные продукты нельзя модифицировать прямым воздействием вручную на эти продукты.

8.5.7 Продукты необходимо регенерировать, если что-то нужно модифицировать, например, относительно результатов деятельности по экспертизе или верификации.

8.6 Документация

В настоящем подразделе приведены общие требования к документации для проектирования и реализации HPD. Настоящий подраздел дополняет требования, характерные для конкретных мероприятий, рассматриваемых в 8.1—8.5.

8.6.1 Конец этапов проектирования и реализации необходимо обозначить выработкой спецификации проекта HPD.

Спецификация проекта HPD служит основой формальной экспертизы проектирования, реализации и последующего изготовления.

8.6.2 Необходима достаточно подробная документация, чтобы изготовление могло идти без дальнейшего разъяснения.

8.6.3 Документ следует структурировать согласно этапам процесса разработки. Спецификация проекта может быть выражена как один документ или как комплексный набор документов.

8.6.4 В случае если используют большое количество документов, то каждый документ должен обладать определенным соотношением с другими документами и содержать ограниченный предмет рассмотрения.

8.6.5 Форматы документации следует отбирать согласно конкретным темам, включая:

a) повествовательное описание;

b) арифметические и логические выражения;

c) графические представления, диаграммы и рисунки.

8.7 Экспертиза проекта и реализации

8.7.1 Этап проектирования и реализации необходимо завершить формальной экспертизой.

8.7.2 В ходе экспертизы и реализации проекта необходимо изучить документацию, охватывающую проектирование, реализацию, анализ и верификации.

8.7.3 При экспертизе необходимо исследовать полноту и правильность файлов параметров и ограничений, предоставляемых инструментам проектирования и реализации.

8.7.4 При экспертизе необходимо исследовать полноту и правильность STA и пост-трассировочного анализа, чтобы проверить правильность и робастность конструкции и реализации с учетом потенциальных отрицательных эффектов, вызванных модификациями, выполненными при помощи инструментов (таких, как упрощение логики или дублирование логического элемента).

8.7.5 В комиссию необходимо включить экспертов и инженеров по аппаратным средствам из коллективов, ответственных за систему или элементы, которые используют HPD или сопряжены с ним (такие, как электронная плата или программное обеспечение).

9 Верификация HDL-программируемого устройства

9.1 Общие положения

Деятельность по верификации, осуществляемая в рамках разработки HPD, является ответственностью изготовителя оборудования контроля и управления и осуществляется персоналом, независимым от персонала, занятого в проектировании и реализации HPD. Самый адекватный путь состоит в том, чтобы привлечь группу верификации.

Возможны дополнительные мероприятия по верификации в рамках сторонней оценки HPD и процесса его разработки для гарантии того, что HPD достигнет планируемых показателей. Существует много способов обеспечения ресурсами и проведения независимой верификации, при этом, как правило, данный вопрос является вопросом предпочтений государственного регулирующего органа.

9.1.1 В группу верификации необходимо включить специалистов, не занятых в разработке и обладающих необходимым профессионализмом и знанием. Уровень требуемой независимости устанавливают нижеследующие требования.

9.1.2 Управление группой верификации должно быть отдельным и независимым от управления группой разработки.

9.1.3 Информационное взаимодействие между группой верификации и группой разработки, для разъяснения или сообщения о неисправности, необходимо проводить формально в письменной форме на таком уровне детализации, который можно проверить в ходе аудита.

9.1.4 Взаимодействия между указанными сторонами следует нацелить на поддержку независимости суждения группы верификации.

9.1.5 Необходимо четко определить ответственность и обязательства группы верификации.

9.1.6 Выходные результаты каждого этапа разработки (см. рисунок 2) необходимо верифицировать.

9.1.7 В ходе мероприятий по верификации необходимо подтвердить адекватность спецификации требований к HPD по выполнению требований к системе или подсистеме, установленных для HPD в связи со спецификацией подсистемы или системы.

9.1.8 В ходе проведения мероприятий по верификации необходимо подтвердить адекватность выбора и правил использования каждой заготовки интегральной схемы, микроэлектронной технологии, конфигурируемого блока и PDB при выполнении спецификации требований к элементу (см. раздел 7).

9.1.9 В ходе проведения мероприятий по верификации необходимо подтвердить адекватность проектной спецификации HPD в выполнении спецификации требований к HPD.

9.1.10 В ходе проведения мероприятий по верификации необходимо подтвердить соответствие HPD проектной спецификации HPD (см. раздел 8).

Примечание — Верификация после реализации имеет первостепенное значение для обнаружения потенциально неблагоприятных последствий упрощений логики и дублирований логических элементов, которые могут быть выполнены инструментами, а также потенциальных отказов, вызванных непосредственно инструментами или их использованием.

9.1.11 Каждое производственное мероприятие следует начинать на основе верифицированных входных данных/документов.

9.1.12 Верификацию продукта следует выполнять перед началом следующего этапа. В противном случае данную верификацию необходимо проводить перед верификацией следующего этапа. Допускается возможную подготовительную работу для последующего этапа сделать до того, как будет верифицирован предыдущий этап.

9.1.13 Если входные данные/документы для мероприятия изменены, то необходимо повторить данное мероприятие и последующие мероприятия по мере необходимости для решения проблем потенциального влияния.

9.2 План верификации

9.2.1 Необходимо составить план верификации до начала мероприятий по верификации HPD.

9.2.2 В плане верификации необходимо документально зафиксировать все критерии, методики и инструменты, которые будут использованы в процессе верификации.

9.2.3 В плане верификации необходимо описать мероприятия по оценке каждого элемента HPD, каждого инструмента, участвующего в процессе разработки, и каждого этапа для того, чтобы показать соответствие спецификации требований HPD.

9.2.4 Необходима такая степень детализации плана верификации, чтобы группа верификации могла выполнить его и достигнуть объективного суждения о том, соблюдает ли HPD спецификацию требований.

9.2.5 План верификации разрабатывает группа верификации и включает в план:

a) выбор и обоснование стратегий верификации согласно типу требований, характеристикам проектирования, реализации и микроэлектронной технологии;

b) выбор и использование инструментов верификации;

c) проведение верификации;

d) документацию по мероприятиям верификации;

e) оценку результатов верификации, полученных непосредственно от инструментов верификации и на основании результатов испытаний, оценку того, соблюдены ли требования по обеспечению безопасности.

9.2.6 В плане верификации необходимо документально зафиксировать каждое испытание, включая его цель, ожидаемые результаты и критерии принятия решения о правильности результата.

9.2.7 Испытания, разработанные согласно функциональным аспектам, должны привести к обширному функциональному тестированию HPD.

9.2.8 В плане верификации необходимо идентифицировать все объективные признаки, требуемые для подтверждения объема контроля. С этой целью необходимо обосновать и документально зафиксировать критерии тестового покрытия, выбранные согласно проекту и его реализации.

9.2.9 Необходимо адекватно учесть обработку и решение всех проблем обеспечения безопасности, рассматриваемых во время мероприятий верификации, выполняемых либо при разработке изготовителем оборудования контроля и управления, либо при сторонней оценке.

9.2.10 Все проблемы обеспечения безопасности необходимо адекватно решать посредством надлежащих корректирующих модификаций или смягчающих положений.

9.3 Верификация использования предварительно разработанных элементов

Правильную конфигурацию и использование предварительно разработанных элементов, таких как заготовки интегральных схем, конфигурируемые блоки и PDB, а также их взаимную совместимость необходимо проверить на соответствие правилам, установленным изготовителем и разработанным во время мероприятий, приведенных в разделе 7.

9.4 Верификация проекта и реализации

9.4.1 В процесс верификации необходимо включить испытания и анализ для рассмотрения:

a) соответствия между проектной спецификацией и спецификацией требований HPD в отношении согласованности и полноты вплоть до самого нижнего уровня блока и модуля включительно;

b) разложения проекта на иерархию блоков и модулей, а также способа, которым они определены в отношении:

1) контролепригодности для дальнейшей верификации,

2) понятности для групп разработки и верификации,

3) модифицируемости, позволяющей дальнейшую модификацию;

c) правильной реализации требований по обеспечению безопасности;

9.4.2 Результат верификации необходимо документально зафиксировать.

9.4.3 В документацию необходимо включить выводы и четко идентифицировать проблемы, для решения которых требуется определить:

a) объекты, не соответствующие требованиям;

b) объекты, не соответствующие правилам проектирования и реализации;

c) модули, данные, структуры и алгоритмы, слабо адаптированные к проблеме.

9.5 Испытательные стенды

9.5.1 Необходимо разработать и документально зафиксировать программу моделирования и тестирования (испытательный стенд). По мере необходимости данный испытательный стенд может состоять из нескольких реализаций, каждая с разным объемом контроля и целью; например, некоторые испытательные стенды могут быть выделены для модулей, а один или больше — для высокоуровневых испытаний.

9.5.2 Испытательный стенд (структура) может быть разработан коллективом проектировщиков для собственных испытательных потребностей и может использоваться группой верификации. Однако необходимо, чтобы тестовые векторы (входные и ожидаемые выходные сигналы), требуемые настоящим стандартом, были разработаны группой верификации, чтобы снизить потенциал для маскировки ошибок и предоставить дополнительное подтверждение понятности и полноты проектной документации.

9.5.3 Необходимо, чтобы испытательный стенд:

a) функционально тестировал каждый модуль в своей среде, моделируемой со всеми необходимыми логическими деталями;

b) обеспечивал достаточное разрешение по времени при использовании после реализации по временным аспектам.

9.5.4 В испытательный стенд необходимо включить тестовые сценарии, которые тестируют все функциональные средства, упомянутые в спецификации требований к HPD и проектной спецификации, такие как функции, режимы, конечные автоматы, алгоритмы, протоколы.

9.5.5 В испытательный стенд следует включить все необходимые входные данные, последовательности и синхронизации, а также регистрировать все выходные последовательности и синхронизации, получаемые при выполнении, для полной автоматизации выполнения теста.

9.5.6 В испытательный стенд следует включить ожидаемые выходные последовательности и синхронизации, а также автоматизированное сравнение с фактически полученными при выполнении теста (адекватные критерии, см. подраздел 9.2), чтобы обеспечить глобальный результат «пригоден — непригоден» в дополнение к подробным результатам испытаний.

9.5.7 В случае если требуются ручной ввод, наблюдения или сравнения:

a) затрагиваемые данные и мероприятия необходимо документально подробно зафиксировать, чтобы позволить лицам, не занятым в проекте, повторить испытание. Это может потребовать определения пошаговых этапов и битовых значений;

b) необходимо привести документальное обоснование, т. к. ручной ввод, наблюдения и сравнения потенциально подвержены ошибкам.

9.5.8 Испытательный стенд должен точно сообщать обо всех отказах и не давать ложных сообщений об успешном результате. Испытательный стенд необходимо строить в соответствии с 10.4.6 и 15.2.

9.6 Тестовое покрытие

9.6.1 Критерии тестового покрытия необходимо отобрать и документально зафиксировать.

9.6.2 В документально зафиксированном анализе критериев тестового покрытия необходимо показать, что они достаточны в отношении спецификации требований к HPD и характеристик проектирования/реализации и что испытательный стенд обеспечивает достаточную наблюдаемость для принятия решения «пригоден — непригоден» для каждого охваченного элемента.

9.6.3 Отобранные критерии могут быть соотнесены, например, с инструкциями, решениями, выражениями, путями, конечными автоматами или процессами. Если нельзя достигнуть целевого критерия покрытия, например, из-за структуры RTL (100 %-ного покрытия пути особенно трудно достигнуть), то необходимо выработать и документально зафиксировать обоснование.

Примечание — Путь представляет собой специфическую последовательность операций ветвления при выполнении программы.

9.6.4 Каждый модуль, разработанный в рамках проекта, необходимо испытать.

9.7 Выполнение испытаний

9.7.1 Испытания необходимо проводить с помощью испытательных стендов после этапа проектирования на описании RTL для подтверждения его правильности.

9.7.2 Испытания необходимо выполнять после этапа реализации для подтверждения того, что пост-трассировочное описание соответствует ограничениям синхронизации, с учетом информации о синхронизации, получаемой от инструментов и из библиотек (обратное аннотирование).

9.7.3 Испытания (с помощью моделирования) необходимо проводить как для «худшего случая» (максимальная задержка распространения сигнала), так и для «лучшего случая» (минимальная задержка распространения сигнала).

9.7.4 Результаты испытаний (значения, последовательности и синхронизации) необходимо документально фиксировать.

9.7.5 В ходе документально фиксируемого анализа любого расхождения необходимо решить, приемлемо ли оно или нет.

9.8 Статическая верификация

9.8.1 Выполняют следующие мероприятия верификации:

a) проверка типа и синтаксиса;

b) проверка параметров в вызове или инстанцировании модулей, функций, процедур, конфигурируемых блоков и PDB;

c) проверка выхода за пределы диапазона;

d) полнота сигналов запуска процессов (см. примечание);

e) полнота случаев, явно запрограммированных в инструкциях и конструкциях с многочисленными вариантами;

f) обнаружение тупиковых состояний в конечных автоматах;

g) обнаружение побочных эффектов в функциях или макроопределениях, обнаружение объектов общего пользования;

h) логический и физический DRC (проверка проектных норм), который тестирует перечень связей и другие сгенерированные файлы на наличие физических и логических ошибок.

Примечание — «Список сигналов запуска» является элементом VHDL.

9.8.2 Для некоторых аспектов верификации можно использовать методы статической верификации, такие как статический временной анализ (см. 8.4.7), если их принципы математически обоснованы. В этом случае инструменты, используемые для реализации этих методов, должны:

a) быть проверенными и стандартизованными, подобными требуемым настоящим стандартом для инструментов моделирования;

b) соответствовать требованиям раздела 15, применимым к инструментам верификации.

10 Аспекты системной интеграции HDL-программируемого устройства

10.1 Общие положения

Процесс системной интеграции — это объединение верифицированных элементов аппаратных средств (и программного обеспечения в применимых случаях) в подсистемы и, наконец, в полную систему. Данный процесс состоит из двух видов деятельности:

a) системная интеграция: сборка и соединение верифицированных аппаратных элементов (и элементов программного обеспечения, в применимых случаях) для построения промежуточных и заключительных целевых объектов. Последовательность сборки, а также степень интеграции последовательных целевых объектов зависят от проектных характеристик;

b) верификация интегрированной системы: подтверждение того, что элементы соответствуют своей проектной спецификации, способны работать совместно и соответствуют требованиям к интерфейсу.

В настоящем разделе приведены требования к системной интеграции в дополнение к МЭК 61513 (пункт 6.2.5) в случае, когда фигурируют HPD.

10.2 Аспекты плана системной интеграции для HDL-программируемого устройства

Настоящий подраздел ужесточает требования МЭК 61513 (пункт 6.3.4).

10.2.1 План системной интеграции для HPD необходимо разработать и документально зафиксировать на этапах проектирования и реализации и верифицировать в отношении требований к системам класса 1.

10.2.2 Данный план необходимо подготовить заранее в процессе разработки, чтобы гарантировать то, что все требования к интеграции включены в проект HPD, системы и ее элементов.

10.2.3 В данном плане необходимо указать стандарты и процедуры, обязательные к выполнению на этапе системной интеграции.

10.2.4 В данном плане необходимо документально зафиксировать те положения плана обеспечения качества системы, которые применимы к системной интеграции.

10.2.5 В плане системной интеграции для HPD необходимо указать:

a) последовательности и синхронизации входных сигналов в проверяемой системе или подсистеме;

b) последовательности и синхронизации ожидаемых выходных сигналов из проверяемой системы или подсистемы;

c) критерии обоснования применения.

10.2.6 В плане системной интеграции необходимо учесть требования, которые должно выполнять HPD, посредством проектирования системы, проектирования аппаратных средств и проектирования программного обеспечения. В план необходимо также включить требования к процедурам и методам управления, охватывающим:

a) управление конфигурацией системы (см. 5.5);

b) системную интеграцию;

c) верификацию интегрированной системы;

d) устранение отказов.

10.2.7 В плане системной интеграции необходимо определить как аспекты идентификации, так и аспекты контроля в управлении конфигурацией согласно требованиям МЭК 61513 (подпункт 6.3.2.3).

10.2.8 В процессе верификации взаимодействия HPD с другими элементами системы определенные аспекты можно верифицировать на уровне подсистем (вычислительных блоков) или на уровне полной системы, если это более практично. В случае если верификация путем тестирования на этих уровнях невозможна, то:

a) все требования HPD необходимо верифицировать другими средствами (например, тестирование по исходным текстам);

b) соответствующую стратегию верификации необходимо документально зафиксировать в плане интеграции.

10.2.9 Все взаимозависимости между верификацией HPD и верификацией интегрированной системы необходимо документально зафиксировать в плане системной интеграции.

10.3 Специфические аспекты системной интеграции

Специфические процедуры для системной интеграции зависят от характеристик архитектуры системы.

10.3.1 Необходимо установить процедуры и сослаться на них в плане системной интеграции для охвата следующих мероприятий:

a) приобретение правильных элементов согласно плану управления конфигурацией системы (МЭК 61513, 6.3.2.3) и процедурам производства (раздел 13);

b) интеграция HPD в систему (например, расположение элементов, конфигурация, межсоединения);

c) предварительное функциональное испытание функций интегрированной системы (см. требования, приведенные ниже);

d) документирование результатов интеграционного процесса и конфигурации системы, подвергнутых испытаниям;

e) формальный релиз интегрированной системы для тестирования пригодности.

10.3.2 Если устранение отказа требует модификации в проверенном HPD или проектной спецификации, то об этом отказе нужно сообщить согласно процедурам, установленным в 10.5.

10.3.3 Любые отказы, обнаруженные во время системной интеграции, которые являются лишь ошибками непосредственно в интеграционном процессе и которые не затрагивают каких-либо документов HPD, необходимо исправлять путем обновления плана системной интеграции.

10.4 Верификация интегрированной системы

Верификация интегрированной системы определяет, должным ли образом объединены в систему верифицированные элементы и подсистемы, совместимы ли и функционируют ли они как положено.

10.4.1 Необходимо, чтобы система была полной в максимально практичной степени для данной верификации.

10.4.2 Необходимо, чтобы тестовые сценарии, отобранные для верификации системы:

a) тестировали все интерфейсы HPD и все основные операции;

b) тестировали все характеристики интерфейса HPD, приведенные в спецификации требований и в проектной спецификации, такие как протоколы, последовательности, синхронизации и электрические функции;

c) обладали достаточным покрытием, позволяющим подтвердить, что HPD функционирует на требуемом уровне для всех достижимых в системе случаев.

10.4.3 План системной интеграции должен идентифицировать выполняемые тесты для каждого требования к интерфейсу HPD.

10.4.4 Необходимо, чтобы группа верификации с хорошим знанием спецификации системы рассмотрела программу испытаний интегрированной системы и оценила результаты испытаний.

10.4.5 Оборудование, используемое для верификации системы, необходимо надлежащим образом калибровать.

10.4.6 Необходимо, чтобы используемые программные инструменты верификации соответствовали требованиям раздела 15, рассматривающего инструменты верификации.

10.4.7 В ходе верификации интегрированной системы необходимо показать, что все элементы системы обладают адекватными эксплуатационными характеристиками (например, блоки обработки и устройства связи).

10.5 Процедуры устранения отказа

10.5.1 Необходимо применять требования МЭК 61513 (подпункт 6.3.2.4) («Процедуры устранения отказа»).

10.5.2 Процедуры устранения отказа должны гарантировать, что любая необходимая модификация HPD соответствует требованиям раздела 12.

10.6 Аспекты отчета об испытании интегрированной системы с HDL-программируемым устройством

10.6.1 Необходимо применять требования МЭК 61513 (подпункт 6.4.5.2).

10.6.2 Результаты испытаний необходимо сохранять в форме, позволяющей их верификацию специалистами, не занятыми непосредственно в разработке плана верификации или в фактическом выполнении тестирования.

11 Аспекты валидации системы с HDL-программируемыми устройствами

11.1 Общие положения

Валидацию HPD, как правило, проводят в рамках этапа валидации системы. Валидация системы рассмотрена в МЭК 61513. Настоящий стандарт устанавливает дополнительные требования к валидации эксплуатационных характеристик (функциональных, временных и электрических) HPD.

a) В соответствии с требованиями к системам класса 1 для валидации системы и HPD необходимо провести испытания.

b) Валидационные испытания необходимо провести на системе в конфигурации ее финальной сборки, включая окончательную версию HPD.

11.2 Аспекты плана валидации системы с HDL-программируемыми устройствами

11.2.1 Валидацию системы необходимо проводить в соответствии с формальным планом валидации системы.

11.2.2 В плане следует определить статические и динамические тестовые сценарии.

11.2.3 Необходимо разработать план валидации системы, а результат валидации должны оценить специалисты, не участвующие в проектировании и реализации.

11.3 Валидация системы

11.3.1 Систему необходимо тестировать с помощью статических и динамических входных сигналов, имитирующих нормальную эксплуатацию, ожидаемые при эксплуатации события и аварийные условия, требующие действий.

11.3.2 Каждую функцию категории А системы необходимо тестировать набором испытаний, подтверждающих каждый необходимый выходной сигнал одиночным или комбинированным способом.

11.3.3 При испытаниях необходимо:

a) охватывать все функции спецификации требований HPD во всех режимах (см. 6.2);

b) охватывать все диапазоны сигналов и расчетных параметров, если для этого имеется весомое основание;

c) охватывать мажоритарную логику, другую одиночную или комбинированную логику;

d) испытывать все сигналы аварийного отключения или защитные сигналы в конфигурации окончательной сборки;

e) охватывать необходимую реакцию на указанные отказы;

f) охватывать все прочие функции, оказывающие влияние на безопасность реактора.

11.3.4 Кроме того, значения входных сигналов, ожидаемые выходные сигналы и критерии обоснования применения необходимо указать в плане валидации системы.

11.3.5 Оборудование, используемое для валидации, необходимо соответственно калибровать и конфигурировать (параметры аппаратуры и программного обеспечения).

11.4 Аспекты отчета о валидации системы с HDL-программируемыми устройствами

11.4.1 В отчете о валидации системы необходимо документально зафиксировать результаты испытаний, связанные с HPD, включенным в систему.

11.4.2 В отчете необходимо идентифицировать аппаратные средства, программное обеспечение, при необходимости, используемую конфигурацию системы, используемые конфигурации инструмента и используемое испытательное оборудование (включая его калибровку и имитационные модели) в соответствии с МЭК 61513 (перечисление b 6.4.6.2).

11.4.3 В отчете необходимо также идентифицировать любые расхождения, выявленные при испытании.

11.4.4 Данный отчет должен подытоживать результаты валидации системы.

11.4.5 Данный отчет должен оценивать соответствие системы всем требованиям.

11.4.6 Результаты необходимо сохранить в форме, позволяющей их верификацию специалистам, не занятым непосредственно в валидации.

11.4.7 Моделирования станции и ее систем, используемые для валидации, необходимо документально зафиксировать.

11.5 Процедуры устранения отказа

Требования 10.5 также необходимо применять к аспектам валидации системы, связанным с HPD.

12 Модификация

12.1 Модификация требований, конструкции или реализации

12.1.1 Необходимо, чтобы процесс модификации и документация соответствовали требованиям МЭК 61513 (пункты 6.2.8 и 6.4.7), МЭК 60987:2007 (раздел 12) и МЭК 60880:2006 (раздел 11).

12.1.2 Все затрагиваемые документы должны проверить согласно требованиям раздела 9 специалисты, не занятые в проектировании или реализации модификации.

12.2 Модификация микроэлектронной технологии

Поставщик может обновить микроэлектронную технологию (например, новая версия заготовки FPGA, чтобы увеличить быстродействие или уменьшить размер кристалла). Даже если новая часть заявлена как «совместимая», это не является гарантией того, что любая данная конструкция будет функционировать тождественно на обоих устройствах.

12.2.1 Процесс обоснования применения (см. раздел 7) необходимо выполнить снова, сопроводив в случае необходимости всеми затрагиваемыми этапами жизненного цикла в зависимости от выявленных различий.

12.2.2 Необходимо снова выполнить соответствующие мероприятия по верификации и должным образом их документально зафиксировать, чтобы гарантировать соблюдение всех функциональных, электрических требований и требований синхронизации.

12.2.3 Даже если новые и старые части имеют одинаковую логическую конфигурацию и совместимы по выводам, то нужно оценить и документально зафиксировать необходимость повторной генерации программных файлов (например, из-за вариаций в синхронизации или напряжениях программирующих импульсов).

13 Производство HDL-программируемого устройства

13.1 Общие положения

Область применения настоящего стандарта исключает проектирование и изготовление предварительно разработанных микроэлектронных ресурсов (например, заготовок FPGA), используемых процессом разработки HPD в качестве входных данных. В настоящем стандарте термин «производство» обозначает заключительные этапы, которые поставляют готовую к использованию интегральную схему в систему контроля и управления.

13.2 Производственные испытания

13.2.1 При проведении испытаний необходимо проверить функции HPD, а также его временны́е характеристики (такие, как частота, время подъема и спада, время распространения и т. д.) и электрические характеристики (такие, как энергопотребление, емкости и т. д.).

13.2.2 Следует подтвердить, что испытания, выполненные изготовителем интегральной схемы, соответствуют требованиям 13.2.1. Производителю оборудования контроля и управления не обязательно повторять испытания, выполненные изготовителем интегральной схемы, и знать соответствующие тестовые векторы.

13.2.3 Если не выполнены требования 13.2.2, то производителю оборудования контроля и управления необходимо провести дополнительные испытания (с документально зафиксированными входными сигналами, ожидаемыми выходными сигналами и критериями обоснования применения), чтобы выполнить все требования (см. 13.2.1).

13.2.4 При производственных испытаниях, выполняемых на уровне плат (после сборки HPD на печатной плате, например, посредством пайки), необходимо проверить, что интерфейс данной части работоспособен (например, испытание на отказ типа «константная ошибка контакта/вывода», глобальное функциональное испытание).

13.2.5 Каждая изготовленная часть должна пройти производственные испытания или должна быть отклонена.

13.2.6 Результаты испытаний необходимо хранить вместе с идентификационной информацией, такой как номер партии для диагностики потенциальных технологических проблем.

13.3 Программирующие файлы и программирование

13.3.1 Необходимо, чтобы программирующие файлы содержали программы обнаружения ошибок, а программирующее оборудование их проверяло.

13.3.2 Для каждой изготовленной части необходимо:

a) проверить конфигурацию после программирования;

b) сохранить соответствующую информацию о контролепригодности, такую как номер партии, файл системного журнала программирования, характеристики программируемых переключателей до и после программирования.

13.3.3 Необходимо соблюдать все процедуры и требования, установленные изготовителем интегральной схемы (например, для предотвращения электростатического разряда).

13.3.4 Необходимо использовать только те программные инструменты, на которые изготовитель интегральной схемы дает гарантию и обеспечивает их поддержку.

14 Аспекты монтажа, ввода в эксплуатацию и эксплуатации HDL-программируемого устройства

a) Необходимо, чтобы процесс и документация для монтажа, ввода в эксплуатацию и эксплуатации соответствовали требованиям МЭК 61513 (пункты 6.2.7 и 6.3.6), МЭК 60987:2007 (разделы 10 и 13) и МЭК 60880:2006 (раздел 12).

b) В соответствии с МЭК 60671 системы контроля и управления и оборудование, выполняющее функции категории А, периодически подвергают испытанию для подтверждения надлежащего функционирования. Для достижения необходимого тестового покрытия для HPD следует использовать адекватные методики испытаний в целях повышения контролепригодности, например периферийное сканирование.

15 Инструментальные программы для разработки HDL-программируемых устройств

15.1 Общие положения

К инструментальным программам, применяемым при разработке HPD, необходимо применять требования, установленные в МЭК 60880:2006 (раздел 14), за исключением требований 14.3.4.3, 14.3.4.4 и 14.3.4.5.

Примечание 1 — Техническая оценка компании — поставщика программы (не ограниченная гарантией качества) является приемлемым методом для выполнения требования МЭК 60880:20061 (пункт 4.2.2) при условии, что доступна соответствующая документация.

Примечание 2 — Термин «надежность» инструментальных программ, используемый в МЭК 60880:2006 (раздел 14), в настоящем стандарте означает «достоверность» или «правильность».

Примечание 3 — ИСО/МЭК 9126 заменен на ИСО/МЭК 25000.

Примечание 4 — Библиотеки, интегрированные в инструментальные программы, могут быть оценены в контексте оценки инструментальных программ.

Примечание 5 — Верификация выходных сигналов инструментальной программы, рассмотренная в МЭК 60880:2006 (подпункт 14.3.2.4), может быть выполнена различными способами, например моделированием с помощью имитатора, отличного от комплекта основного комплекта инструментальных средств.

15.2 Дополнительные требования к инструментам проектирования, реализации и моделирования

15.2.1 Необходимо, чтобы инструментальные программы предоставляли доступ к параметрам, управляющим логическим синтезом и реализацией (например, через настройки).

15.2.2 Инструментальные программы не должны добавлять структуры, не прослеживаемые непосредственно до исходных операторов HDL (например, дублирование логического элемента для соответствия требованию синхронизации) без предупреждения.

15.2.3 Проектировщики должны обладать ранее полученным знанием инструментальных программ; в частности, они должны знать, как программы функционируют на структурах и конструкциях, используемых в проекте.

15.2.4 Если инструментальная программа требует аргументов командной строки, то необходимо их наличие в файле сценария (размещены под управлением конфигурацией) для избежания ошибок ручного вызова.

Примечание 1 — Вышеизложенное полезно не только для согласованности, но и для оценки происхождения отказа, который может быть в исходном коде, в программе или в параметрах программы, а также для оценки потенциала CCF, обусловленного инструментами проектирования и реализации.

15.2.5 При переходе на новую версию инструментальной программы, которая отвечает за преобразование проектной информации (например, логический синтез или размещение и трассировка), все затрагиваемые мероприятия по моделированию, анализу и верификации необходимо выполнить заново.

Примечание 2 — Можно обосновать в ходе документируемого анализа, что данная модификация программы не может затронуть вышеупомянутую деятельность, например коррекцию некоторого несогласованного поведения в графическом пользовательском интерфейсе программы.

Примечание 3 — Мероприятия, которые были завершены до изменения программы, не нужно повторять.

16 Сегментация или разделение конструкции

16.1 Вводные сведения

На некоторых HPD возможны проектирование и реализация схем, изолированных с помощью физически различных зон интегральной схемы и имеющих минимальные связи или их полное отсутствие и

не использующие общие аппаратные ресурсы. Некоторые HPD поддерживают такие зоны, иногда называемые «озерами», с неиспользованным/непригодным пространством между ними. Некоторые преимущества сегментации или разделения конструкции могут включать в себя реализацию вспомогательных или поддерживающих функций (что не должно быть заменой для резервированных каналов/цепочек в конструкции на системном уровне).

16.2 Вспомогательные функции или функции поддержки

16.2.1 Общие положения

Вспомогательные функции или функции поддержки, реализованные на HPD, даже если они не относятся к функциям категории А, обладают потенциалом влиять на функции категории А данного HPD. Таким образом, если нельзя подтвердить, что требования 16.2.2 соблюдены, то необходимо разработать, реализовать и верифицировать вспомогательные функции или функции поддержки в соответствии с требованиями настоящего стандарта (то есть как функции категории А).

16.2.2 Разделение вспомогательных функций или функций поддержки, отличных от категории А

Настоящий стандарт подтверждает, что при применении специфичных мер проектирования и разделения HPD можно гарантировать, что вспомогательные функции или функции поддержки независимы от функций категории А и не могут ненадлежащим образом влиять на выполнение функций категории А. При соответствии требованиям, приведенным в перечислениях a) — h), вспомогательные функции или функции поддержки можно реализовать на HPD класса 1 без той степени строгости, которая требуется для функций категории А:

a) необходимо продемонстрировать при помощи конструкции, реализации, оценки и систематической верификации то, что эксплуатация или отказ данных вспомогательных функций или функций поддержки не могут влиять прямо или на выполнение какой-либо функции категории А, независимо от того, является ли причина отказа внутренней или внешней по отношению к HPD (например, вызвана источниками электропитания, коротким замыканием на подключенной линии и т. д.);

b) данная демонстрация должна рассматривать все потенциальные причины помех, например функциональные, электрические, электромагнитные, тепловые и т. д.;

c) в частности, зоны интегральной схемы, используемые для реализации таких вспомогательных функций или функций поддержки, должны физически отличаться от используемых для реализации функций категории А;

d) в случае модификации HPD следует подтвердить, что требования 16.2.2 все еще соблюдаются;

e) необходимо, чтобы интерфейс между схемами, реализующими функции категории А и вспомогательные функции или функции поддержки, был простым и полностью верифицируемым;

f) данные, полученные функциями категории А от вспомогательных функций или функций поддержки, необходимо ограничить значениями статических параметров (например, константы калибровки, уставки);

g) функции категории А не должны обладать временной зависимостью от получения данных от вспомогательных функций или функций поддержки;

h) необходимо реализовать адекватные меры безопасности (например, безопасные протоколы связи) для любого информационного взаимодействия между функциями категории А и вспомогательными функциями или функциями поддержки таким образом, чтобы обнаружить все ошибки передачи данных и предпринять подходящие безопасные меры реагирования или подтвердить правильное получение данных.

17 Защита от отказа по общей причине в HDL-программируемом устройстве

17.1 Вводные сведения

Систематические отказы могут возникнуть в любом процессе проектирования и реализации из-за ошибки персонала; и, следовательно, такие отказы могут возникнуть во время проектирования и реализации HPD (либо в разработанной части, либо во включенной существующей ранее конструкции). Следовательно, на HPD потенциально могут повлиять скрытые систематические отказы, которые при возникновении некоторых инициирующих событий могут привести к CCF при создании многочисленных экземпляров класса конструкции HPD.

Потенциал возникновения CCF в многоэлементных системах рассмотрен в стандартах ПК 45А более высокого уровня, в частности МЭК 61513 и МЭК 62340. Потенциал возникновения CCF, обусловленных созданием множественных экземпляров конструкции HPD в данной системе, рассматривается в настоящем стандарте. Как указано в разделе 1 «Область применения», настоящий стандарт устанавливает требования к разработке и верификации и требования, которые минимизируют потенциал для систематических отказов HPD, и таким образом — поскольку такие отказы могут вызвать ООП — также минимизируют потенциал для CCF, обусловленных HPD.

В 17.2 приведены дополнительные требования, нацеленные на защиту от систематических отказов, которые могут привести к CCF, обусловленным HPD.

17.2 Требования

17.2.1 Аспекты процессов разработки HPD, которые могут привести к CCF множественных экземпляров конструкции HPD (и которые не рассмотрены в настоящем стандарте), должны соответствовать, в зависимости от применимости, требованиям МЭК 60880:2006 (подраздел 13.1) (заменяя «программное обеспечение» на «HPD»).

Примечание 1 — Указанные аспекты, как правило, связаны с разработкой программ на HDL.

17.2.2 В зависимости от применимых требований необходимо выполнить анализ согласно требованиям МЭК 60880:2006 (пункты 13.3.1–13.3.4, 13.3.7–13.3.8), чтобы рассмотреть аспекты процессов разработки HPD, которые могут привести к CCF множественных экземпляров конструкции HPD (и которые ранее не были рассмотрены в настоящем стандарте).

Примечание 2 — Некоторые требования этих подпунктов рассматривают CCF в системах на уровне архитектуры контроля и управления, хотя лучше их расположить в стандарте высшего уровня, посвященном CCF, МЭК 62340. В целях сохранения структуры стандартов серии ПК 45А предлагается перенести эти требования в МЭК 62340 при следующей актуализации стандарта.

Приложение А
(справочное)

Документация

Настоящее приложение определяет типичную документацию для каждого из разделов настоящего стандарта. Содержимое можно организовать в набор документов, отличающихся от предложенных в настоящем приложении, при условии, что разделы четко идентифицированы.

А.1 Проект

a) план управления проектом;
b) план обеспечения качества;
c) план управления конфигурацией.

А.2 Спецификация требований к HDL-программируемому устройству

a) спецификация требований;
b) отчет по анализу требований;
c) акт.

А.3 Обоснование применения заготовок интегральных схем, конфигурируемых блоков и предварительно разработанных блоков

a) спецификация требований к элементу;
b) пользовательская документация по безопасности;
c) прочая документация к элементу, включая любую информацию, такую как спецификация, конструкция, испытание, опыт эксплуатации;
d) отчет по анализу;
e) документ, содержащий правила использования;
f) отчет по анализу результатов обоснования применения.

А.4 Проектирование и реализация HDL-программируемого устройства

a) спецификация проекта, включая:
1) описание: разбивки на основные модули, опции защитного проектирования, идентификации микроэлектронной технологии, инструментов, конфигурируемых блоков и PDB;
2) описание рабочего проекта, включая:
- описание на RTL;
- организационные опции (модули, подмодули, интерфейсы, протоколы и т. д.);
- предварительные электрические характеристики и синхронизации;
3) описание реализации, включая:
- описание на уровне логических элементов (список связей), специальное технологическое описание для производства, обратное аннотирование;
- реализация модулей, критических сигналов и распределения электропитания, опций инструментов, вспомогательных файлов, используемых для реализации, таких как «файлы ограничений»;
- отчет по пост-трассировочному анализу, отчет по STA;
- анализ контролепригодности, тестовые векторы для периодических испытаний;
- электрические характеристики и подробные синхронизации;
b) отчеты, акты.

А.5 Верификация HDL-программируемого устройства

a) план верификации;
b) документ, содержащий: описание испытательного стенда, критерии покрытия, тестовые сценарии;
c) документ, содержащий анализ и обоснование критериев покрытия;
d) отчет, включающий в себя: результаты испытаний и анализа (на уровне RTL, после синтеза, пост-трассировочный), анализ соблюдения правил использования.

А.6 Аспекты системной интеграции HDL-программируемого устройства

a) план интеграции, включающий в себя: стратегию и процедуры интеграции, интерфейс управления конфигурацией, тестовые сценарии;
b) специфичные аспекты отчета об испытании интегрированной системы, включая идентификацию элементов и инструментов, результаты испытаний и анализа, обнаруженные отказы и их устранение;
c) отчет и акты интеграции.

A.7 Аспекты системной валидации HDL-программируемого устройства

a) план валидации, включая тестовые сценарии;

b) отчет, включающий в себя: идентификацию элементов и инструментов, результаты испытаний, анализ результатов испытаний, обнаруженные отказы и их устранение.

A.8 Модификация

В МЭК 60880 (приложение F) приведен типичный перечень документации, связанной с процессом модификации:

a) отчет об аномалиях;

b) запрос на модификацию;

c) отчет о модификации;

d) архив управления модификациями.

Кроме того, необходимо актуализировать документы, связанные с этапами разработки, затрагиваемые модификацией.

A.9 Производство HDL-программируемого устройства

a) документ, содержащий описание производственных испытаний;

b) документ, содержащий результаты производственных испытаний, часть идентификационной информации и часть программной информации.

A.10 Инструментальные программы для разработки HDL-программируемых устройств

a) отчет о выборе инструментальной программы (анализ поддержки выбранной инструментальной программы, оценка, соответствие требованиям, пределы применимости);

b) документ, излагающий стратегию модификации, обновления или замены.

Приложение В
(справочное)

Разработка HDL-программируемых устройств

Мероприятия по разработке HPD, рассматриваемые в настоящем стандарте, основаны на языках описания аппаратуры и инструментах проектирования, функционирующих на рабочих станциях, согласно порядку операций, представленному в приложении для упрощения понимания соответствующих разделов настоящего стандарта.

В.1 Факультативное определение требований на уровне электронных систем

Требования устанавливают на основании высокоуровневого описания системы, к которой принадлежит HPD. Каждый элемент системы представлен моделью его поведения, и данные модели осуществляют обмен информацией по каналам связи, имитируя проектируемую систему.

Данный уровень описания, называемый «уровнем электронной системы» или ESL, использует языки описания системы, такие как SystemC или System Verilog.

Данное описание, как правило, выполняют (моделируют) с помощью функциональных тестовых сценариев для оценки адекватности различных системных архитектур, выбора наилучшей и окончательной установки требований к каждому элементу, включая HPD, исходя из динамических характеристик и интерфейса.

В.2 Проектирование

Начиная с формулировки требований деятельность по разработке изначально нацелена на определение основных принципов проектирования, таких как разделение на предварительно разработанные или заказные модули, организацию самоконтроля и идентификацию микроэлектронной технологии (включая конфигурируемые блоки) и PDB, которые могут быть использованы.

Затем строят описание на RTL (Register Transfer Level — уровень регистровых передач). Используют такие языки описания аппаратуры, как VHDL или Verilog. В основном это не зависит от используемой микроэлектронной технологии.

Данное высокоуровневое описание представляет собой синхронную параллельную модель HPD, описывающую его поведение посредством сигналов, преобразуемых комбинационными функциями и последовательно передаваемых между регистрами, инициируемыми одним или несколькими генераторами тактовых сигналов.

Описание на RTL обладает структурными аспектами, показывающими логические связи между модулями, которые можно специально спроектировать или взять из библиотек. Описание на RTL также обладает поведенческими аспектами, позволяя использовать алгоритмическое описание функций модуля. Данное описание выполняют посредством некоторого HDL (языка описания аппаратуры), как правило, VHDL (IEEE 1076) или Verilog (IEEE 1364).

Необходимо, чтобы описание на RTL было синтезируемым, что означает возможность его автоматической трансляции в набор взаимосвязанных электронных вентилей. Для достижения этого свойства проектировщик использует лишь подмножество языка HDL, тогда как полный язык можно использовать, например, для создания сред моделирования.

Параллельно с проектированием считается полезным разработать «испытательный стенд» на том же языке: RTL-описание HPD включают в более широкую программу на HDL, которая отправляет его входные последовательности и считывает его выходные сигналы для испытания посредством моделирования. Испытательный стенд может использовать несинтезируемые языковые функции для упрощения разработки тестов (например, доступ к файлам, печать, явное управление временем). Затем испытательный стенд используют для проверки описания RTL, а также его можно соотнести с различными инструментами для генерации тестов и измерений покрытия.

Для организации подхода дополнительной верификации вводят инструменты статического анализа. Как правило, они позволяют проверить удержание ожидаемых свойств на описании HDL. Примерами статического анализа являются: проверка свойств, верификация на основе утверждений, проверка эквивалентности между различными уровнями проектирования (например, RTL и список связей) или STA.

В.3 Реализация

Начиная с описания на RTL, вырабатывают электронное описание, позволяющее фактическую реализацию выбранной электронной технологии. Основными этапами реализации являются логический синтез и размещение с трассировкой.

Различные семейства элементов, таких как FPGA, стандартные ячейки и т. д., выдают различные предварительные характеристики физического поведения конечного продукта. Таким образом, несмотря на то, что приведенные в настоящем пункте мероприятия по своей сути необходимы, сопутствующие инструменты могут обрабатывать их автоматически или не обрабатывать. Ниже приведен обзор указанных мероприятий для проектирования на основе стандартных ячеек.

Логический синтез преобразует описание на RTL в сеть логических ячеек микроэлектронной технологии, называемую «списком связей». В зависимости от этой микроэлектронной технологии ячейки могут представлять

собой просто элементарные вентили (например, AND, OR) или содержать в себе более крупные функции (например, счетчики).

Несмотря на то, что для синтеза используют инструменты, аналогичные программным компиляторам, проектировщик направляет процесс, предоставляя информацию об ожидаемых характеристиках (таких, как частота синхронизации, задержка между двумя сигналами, энергопотребление) и о том, как обращаться с критическими сигналами, например, тактовыми сигналами. Указанную информацию, как правило, хранят в «файлах ограничений», которые могут быть очень большими. Таким образом, их обработка может быть затруднительной, и ошибка или упущение могут привести к генерации схемы, подверженной неявным невоспроизводимым отказам, которые почти невозможно обнаружить посредством моделирования. Таким образом, верификация файлов ограничений является принципиально важным мероприятием.

На этапе размещения и трассировки определяют физическое местоположение ячеек на кремниевом кристалле и связывают их с учетом технологических ограничений (существование и емкость предопределенных трассировочных каналов), а также ограничений применения (например, максимальная задержка распространения между двумя заданными узлами).

По мере роста числа вентилей между ними появляется все больше взаимосвязей, то есть все большее число взаимосвязей необходимо трассировать на кристалле. Кроме того, требования к скорости, как правило, не позволяют удлинять некоторые тракты. Последнее названное ограничение может привести к изменениям размещения некоторых вентилей, что в свою очередь отражается на всей схеме трассировки. Поиск «наилучшего» решения является очень трудной проблемой, поэтому могут быть найдены лишь приближения с помощью инструментов, которым необходимо использовать усложненные и эволюционные алгоритмы.

Описание после размещения и трассировки создают в формате, который зависит от микроэлектронной технологии. Поскольку на данном этапе известна схема физического расположения, то время распространения можно уточнить с учетом сопротивления и емкости каждого тракта. Как правило, эту информацию используют для обратного аннотирования описания для его моделирования на испытательном стенде с реальным временем распространения для ячеек и межсоединений. Кроме того, поставщик микроэлектронной технологии предоставляет время распространения сигнала для ячеек, включенных в его библиотеку с помощью форматов типа VHDL-VITAL (IEEE 1076.4). Данную информацию о синхронизации включают в описание перечня связей как «обратное аннотирование» и учитывают при моделировании «после реализации».

В дополнение к верификации посредством моделирования «после реализации» инструменты для статического анализа позволяют проверять время распространения (STA: Static Timing Analysis — статический временной анализ, STA) или эквивалентность между различными уровнями описания.

B.4 Типы специализированных интегральных схем (ASIC)

B.4.1 Общие положения

С развитием технологии предлагается много вариантов F, поэтому в настоящем стандарте приведены требования, основанные на принципах, а не на конкретных деталях каждого варианта. В данном пункте приведен обзор основных доступных вариантов (примечание — в промышленности их названия не всегда используют единообразно).

Теоретически любую вычисляемую функцию можно реализовать одним типом тщательно выбранного элементарного логического элемента, такого как «NAND» [«A and B» означает «not (A and B)»]. Следовательно, диапазон функций, которые можно реализовать в данной схеме, существенно зависим от ее размера (число вентилей) и ее внутренней связности, что позволяет более или менее эффективное использование вентилей.

B.4.2 Программируемая логическая матрица (PAL)

PAL представляют собой малоразмерные устройства, как правило, организованные в виде массива OR/AND для реализации логических уравнений, имеющих форму суммы произведений, например, *output = (A and B and not C) or (not B and not C) or (D).*

PAL изготавливают как специализированное изделие, конфигурируя взаимосвязи, как правило, посредством прожига плавких вставок или в некоторых случаях конфигурируя перепрограммируемые переключатели.

Структура AND программируемая, т. е. выражение произведения перед программированием следующее: (*A and not A and B and not B and C and not C, и т. д.*), где каждый член выражения соответствует одному конфигурируемому соединению. Согласно функциональным требованиям ненужные члены удаляют и получают, например, (*A and not C*).

Структура OR фиксирована: входные данные схемы OR — это фиксированное число таких программируемых произведений, например *(A and not C) or (A and not B) or (D).*

Для конфигурации PAL, как правило, используют низкоуровневые языки, такие как PALASM: проектировщик вводит реализуемые логические уравнения, а инструмент переводит их в карту соединений. С такими языками невозможно поведенческое описание, такое как в VHDL или Verilog.

PAL, как правило, предоставляют несколько входов и выходов (например, 10 входов, 8 выходов), и они эквивалентны максимум нескольким сотням вентилей. По причине своего ограниченного размера они не входят в область применения настоящего стандарта.

B.4.3 Программируемая логическая интегральная схема, сложная программируемая логическая интегральная схема (PLD, CPLD)

PLD и CPLD представляют собой значительные по размеру массивы взаимосвязанных PAL, но новые семейства могут предлагать дополнительные свойства.

Подобно PAL они основаны на сумме произведений с фиксированной структурой, поэтому трассировка сигнала от входа до выхода фиксирована, а время задержки распространения достаточно постоянно. Разумеется, это свойство может быть утеряно, когда предлагаются дополнительные функции, такие как линии обратной связи или специализированная логика.

Размер СПЛИС достигает эквивалента десятков тысяч вентилей.

B.4.4 Программируемая пользователем вентильная матрица (FPGA)

FPGA организованы как большое число программируемых логических блоков, включая возможности для комбинационной логики и хранения. Данные блоки взаимосвязаны иерархией программируемых межсоединений, а также имеют контактные площадки ввода-вывода (как правило, направление, импеданс, напряжение и сохранение в памяти программируют). Конкретные линии связи, как правило, предназначены для критических сигналов, таких как сигналы синхронизации. Дополнительно FPGA могут содержать специализированные логические блоки, такие как память, ядро процессора, стандартные интерфейсы и т. д.

Вентильная эквивалентность к FPGA не применима, так как их сложные и разнообразные структуры затрудняют прогноз о том, сколько блоков необходимо для данной функции. Некоторые FPGA включают в себя сотни тысяч программируемых блоков, сотни входов/выходов и сделаны из миллиардов транзисторов.

FPGA могут сохранять свои функции («конфигурацию») с помощью таких средств:

a) статическое RAM (конфигурация энергозависимая, копируется при пуске из внешней памяти);

b) флэш-память (конфигурация сохраняется в энергонезависимых, но перепрограммируемых элементах внутренней памяти);

c) антипрожигаемая перемычка (конфигурация постоянна, такие устройства «однократно программируемые»).

Восприимчивость конфигурации к отказу в результате единичного события и нейтронному/альфа-излучению высока для статических RAM, низка для флэш и очень низка для средств с антипрожигаемыми перемычками.

B.4.5 Вентильная матрица или интегральная схема на основе базового матричного кристалла

Поставщик интегральных схем заранее подготавливает стандартные интегральные схемы, в которых все транзисторы уже сделаны, но не взаимосвязаны. Реализуемую конкретную функцию синтезируют в виде конкретной взаимосвязи транзисторов.

Данный подход подразумевает единовременные затраты, связанные с производством специфических масок для металлических слоев (межсоединение), но может предложить более низкую стоимость изготовления детали по сравнению с FPGA, поскольку для реализации программируемой компоновки схем не используется кремний. Тем не менее эту технологию вымещают FPGA.

B.4.6 Стандартные ячейки

Поставщик предлагает микроэлектронную технологию и проектирует с ее помощью ряд стандартных ячеек, таких как элементарные комбинационные логические схемы, триггеры, сумматоры, счетчики и т. д. Данные ячейки обладают известными характеристиками, такими как площадь, входной ток, емкость и задержка распространения сигнала. Ячейки проектируют таким образом, что они обладают одинаковой высотой и различной шириной, поэтому их можно разместить на интегральной схеме рядами для упрощения трассировки и энергоснабжения.

Функциональные и физические характеристики ячеек излагают в технологической библиотеке, которую предоставляют проектировщику I&C. Эту библиотеку используют при логическом синтезе (см. пункт B.3), который преобразует описание на RTL в список связей этих ячеек, которые затем размещают на интегральной схеме и связывают между собой. После завершения функциональных и технологических верификаций изготавливают маски, необходимые для производства интегральных схем, и можно начинать производство.

Данный подход подразумевает более высокие единовременные затраты по сравнению с вентильными матрицами, потому что все маски специфические, но предлагает более низкую стоимость изготовления детали, поскольку интегральная схема будет иметь точно нужный размер. Доступность различных ячеек для каждого типа, оптимизирующих различные аспекты, такие как быстродействие, площадь или энергопотребление, позволяет лучше оптимизировать каждую зону конструкции, оставаясь под управлением проектировщика оборудования контроля и управления только с помощью связанных с HDL инструментов.

B.4.7 Полностью заказная ASIC или необработанная ASIC

Данная технология подразумевает специфичное проектирование всех аспектов интегральной схемы, вплоть до транзисторного уровня, с помощью специализированных инструментов. Это предполагает очень высокие единовременные затраты, требующие больших объемов для экономического обоснования. Данные схемы не входят в область применения настоящего стандарта.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60671	—	*
IEC 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А»
IEC 60987:2007	IDT	ГОСТ Р МЭК 60987—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения для компьютерных систем»
IEC 61513:2011	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
IEC 62138	IDT	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В или С»
IEC 62340	IDT	МЭК 62340—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине»
Руководство МАГАТЭ NS-G-1.3:2002	—	**

*Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

**Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод текста документа на русский язык, который доступен на gost.e-ecolog.ru

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification

[2] IEC 61226, Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions

[3] IEC 62342, Nuclear power plants — Instrumentation and control systems important to safety — Management of ageing

[4] ISO 9001, Quality management systems — Requirements

[5] ISO/IEC 25000, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE)

УДК 621.311.049.75:006.354 ОКС 27.120.20 IDT

Ключевые слова: атомные станции, HDL-программируемое устройство, программируемая логическая интегральная схема, программируемая логическая матрица, программируемая пользователем вентильная матрица, специализированная интегральная схема

Редактор *В.А. Сиволапов*
Технический редактор *В.Ю. Фотиева*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 22.06.2016. Подписано в печать 05.07.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,09. Тираж 25 экз. Зак. 1591.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru