ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62566— 2021

HDL-ПРОГРАММИРУЕМЫЕ УСТРОЙСТВА СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ АТОМНОЙ СТАНЦИИ, ВЫПОЛНЯЮЩИЕ ФУНКЦИИ БЕЗОПАСНОСТИ КАТЕГОРИИ А

Требования к разработке

(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)

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Русатом Автоматизированные системы управления» (АО «РАСУ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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 20 декабря 2021 г. № 1819-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62566:2012 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Разработка HDL-программируемых интегральных схем для систем, 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).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

5 Положения настоящего стандарта действуют в целом в отношении атомных станций, сооружаемых по российским проектам за пределами Российской Федерации

6 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© IEC, 2012
© Оформление. ФГБУ «РСТ», 2022

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 4
5 Общие требования к проектам HPD 5
5.1 Общие положения 5
5.2 Жизненный цикл 5
5.3 Управление проектированием HPD 8
5.4 План обеспечения качества HPD 8
5.5 Управление конфигурацией 8
6 Спецификация требований к HPD 9
6.1 Общие положения 9
6.2 Функциональные аспекты спецификации требований 9
6.3 Детерминированный подход 10
6.4 Выявление дефектов и сохранение работоспособности при наличии дефектов 10
6.5 Определение требований с использованием инструментов на уровне электронной системы . . . 11
6.6 Анализ и пересмотр требований 11
7 Процесс приемки программируемых интегральных схем, встроенных блоков и предварительно разработанных блоков 12
7.1 Общие положения 12
7.2 Спецификация требований к компонентам 12
7.3 Правила использования 13
7.4 Выбор 13
7.5 Обоснование приемки 14
7.6 Внесение изменений для приемки 14
7.7 Внесение изменений после приемки 15
7.8 Документация для приемки 15
8 Проектирование и реализация HPD 15
8.1 Общие положения 15
8.2 Языки описания аппаратных средств (HDL) и сопутствующие инструменты 15
8.3 Проектирование 16
8.4 Реализация 19
8.5 Инструменты системного уровня и автоматизированная генерация кода 22
8.6 Документация 22
8.7 Пересмотр проекта и реализации 23
9 Верификация HPD 23
9.1 Общие положения 23
9.2 План верификации 24
9.3 Верификация использования предварительно разработанных элементов 25
9.4 Верификация проекта и реализации 25
9.5 Стендовые испытания 25
9.6 Тестовый охват 26
9.7 Выполнение испытаний 26
9.8 Статическая верификация 26
10 Аспекты системной интеграции с участием HPD 27
10.1 Общие положения 27
10.2 Аспекты плана системной интеграции с участием HPD 27
10.3 Особые аспекты системной интеграции 28
10.4 Верификация интегрированной системы 28
10.5 Процедуры устранения дефектов 28
10.6 Аспекты отчета о тестировании интегрированной системы, связанные с HPD 29

11 Аспекты валидации системы, связанные с HPD 29
11.1 Общие положения 29
11.2 Аспекты плана валидации системы, связанные с HPD 29
11.3 Валидация системы 29
11.4 Аспекты отчета о валидации системы, связанные с HPD 29
11.5 Процедуры устранения дефектов 30
12 Модификации 30
12.1 Модификация требований, проекта или реализации 30
12.2 Модификация микроэлектронной технологии 30
13 Производство HPD 30
13.1 Общие положения 30
13.2 Производственные испытания 30
13.3 Программирующие файлы и программирование 31
14 Аспекты установки, ввода в эксплуатацию и эксплуатации, связанные с HPD 31
15 Программные средства для разработки HPD 31
15.1 Общие положения 31
15.2 Дополнительные требования к инструментам проектирования, реализации и моделирования . . 32
16 Сегментация или разделение конструкции 32
16.1 Предварительная информация 32
16.2 Вспомогательные функции или функции поддержки 32
17 Защита HPD от отказа по общей причине 33
17.1 Предварительная информация 33
17.2 Требования 33
Приложение А (справочное) Документация 35
Приложение В (справочное) Разработка HPD 37
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 41
Библиография 41

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

HDL-ПРОГРАММИРУЕМЫЕ УСТРОЙСТВА СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ АТОМНОЙ СТАНЦИИ, ВЫПОЛНЯЮЩИЕ ФУНКЦИИ БЕЗОПАСНОСТИ КАТЕГОРИИ А

Требования к разработке

HDL-programmed devices for instrumentation and control systems of a nuclear power plant, performing category A safety functions. Development requirements

Дата введения — 2022—09—01

1 Область применения

1.1 Общие положения

Настоящий стандарт устанавливает требования к разработке высоконадежных программируемых устройств (HDL-Programmed Devices, HPD) для использования в системах контроля и управления (СКУ) атомных станций (АС), выполняющих функции безопасности категории А, классифицированные согласно МЭК 61226.

Программирование HPD выполняют с помощью языков описания аппаратных средств (Hardware Description Languages, HDL) и соответствующих программных инструментов. Как правило, в их основе лежат заготовки программируемых логических интегральных схем (ПЛИС) или подобные микроэлектронные технологии. Интегральные схемы общего назначения, например, микропроцессоры, не относятся к HPD.

Требования, устанавливаемые настоящим стандартом, касаются:

a) специальной разработки жизненного цикла, состоящей в рассмотрении каждого этапа разработки HPD, включая спецификацию требований, проектирование, реализацию, верификацию, интеграцию и валидацию;

b) планировки и дополнительных операций, таких как модификация и производство;

c) выбора предварительно разработанных компонентов, которые включают микроэлектронные ресурсы [например, заготовки программируемых логических интегральных схем (ПЛИС) или сложные программируемые логические устройства (СПЛУ)] и HDL-операторы, представляющие собой предварительно разработанные блоки (ПРБ);

d) применения принципов упрощения и детерминирования, общепризнано имеющих первостепенное значение для достижения безотказной реализации функций категории А;

e) инструментов, используемых для проектирования, реализации и верификации HPD.

Настоящий стандарт не устанавливает требования к разработке микроэлектронных ресурсов, которые обычно являются коммерчески доступными компонентами и не разрабатываются по стандартам, относящимся к обеспечению качества работы ядерных установок. Стандарт обращен к разработкам микроэлектронных ресурсов для проектов СКУ, использующих HDL и соответствующие инструменты.

В настоящем стандарте представлены рекомендации, позволяющие, насколько это возможно, избежать скрытых дефектов, остающихся в HPD, и снижать вероятность единичных отказов и возможных отказов по общей причине (ООП). Требования настоящего стандарта о наличии четкой и полной документации должны способствовать эффективному применению МЭК 62340.

Издание официальное

Настоящий стандарт не рассматривает вопрос надежности квалификации, основанной на воздействии на окружающую среду, а также отказы по причине старения или ухудшения физических характеристик. Эти вопросы рассмотрены в других стандартах, в частности, в МЭК 60987, МЭК 60780 и МЭК 62342.

В подразделе 5.7 МЭК 60880:2006 приведены требования безопасности, относящиеся к разработке HPD в соответствующих случаях.

1.2 Применение настоящего стандарта

Настоящий стандарт содержит рекомендации и требования к HPD для создания верифицируемых проектов и разработок, если при этом необходимо подтверждение их пригодности в отношении, например, выполняемой функции или в связи с важностью ее поведения для безопасности. В СКУ класса 1 могут быть использованы HPD, для которых необязательно полное подтверждение соответствия требованиям настоящего стандарта, например если они не включены в логическую схему, выполняющую функцию безопасности. Однако отклонения от настоящего стандарта следует обосновывать.

В настоящем стандарте рассмотрены действия по разработке HPD, организуемые в рамках определенного жизненного цикла, а также действия и рекомендации, используемые в дополнение к требованиям МЭК 61513 к интеграции и валидации системы при включении HPD в ее состав.

В дополнение к требованиям настоящего стандарта, описывающего HPD, которые входят в состав СКУ класса 1, к ним применимы также требования МЭК 60987, относящиеся к разработке программируемых логических устройств.

Примечание — В случае противоречия требований требования настоящего стандарта имеют преимущество перед требованиями МЭК 60987 в отношении систем класса 1, включающих HPD.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы [для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных — последнее издание (включая все изменения)]:

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

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

IEC 60987:2007[1)], Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems (Электростанции атомные. Контрольно-измерительные приборы и системы управления, важные для обеспечения безопасности. Требования к проектированию аппаратуры для компьютерных систем)

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

IEC 62138[2)], Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (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) (Электростанции атомные. Системы прибор-

[1)] Действует IEC 60987:2021 «Nuclear power plants — Instrumentation and control important to safety — Hardware requirements». Однако для однозначного соблюдения требований настоящего стандарта, приведенного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[2)] Действует IEC 62138:2018 «Nuclear power plants — Instrumentation and control systems important for safety — Software aspects for computer-based systems performing category B or C functions».

ного оснащения и управления, важные для обеспечения безопасности. Требования, позволяющие выдержать отказ по общей причине)

IAEA guide NS-G-1.3:2002[1)], Instrumentation and Control Systems Important to Safety in Nuclear Power Plants (Системы контроля 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.

[МЭК 60050-521:2002, 521-11-18]

Примечание — Специализированную интегральную микросхему проектируют для целей одной компании. В нее закладывают функции, заданные этой компанией.

3.2 **блок** (block): Одна из частей проекта; блок может состоять из других блоков.

Примечание — Блок может быть предварительно разработанным, встроенным или блоком, разработанным в процессе проектирования.

3.3 **отказ по общей причине**[2)]; ООП (Common Cause Failure, CCF): Отказ двух или более конструкций, систем или компонентов вследствие единичного конкретного события или единичной конкретной причины.

[Глоссарий МАГАТЭ по безопасности, 2007 г.]

Примечание — Общие причины могут быть внутренними или внешними по отношению к системе контроля и управления.

[IEC 61513]

3.4 **уровень электронной системы** (Electronic System Level, ESL): Высокоуровневое описание электронной системы, основанное на наборе процессов, представляющих функциональные возможности таких компонентов, как микропроцессоры, память, специализированные вычислительные блоки или каналы связи.

Примечание — Такое описание дает возможность проектировщику разделять систему на компоненты, оценивать ее рабочие характеристики при различных вариантах увязки функций с компонентами и устанавливать требования к компонентам. Описание обычно выполняют с использованием таких языков программирования, как SystemC (IEEE 1666), SystemVerilog (IEEE 1800) или Matlab (R).

3.5 **программируемая логическая интегральная схема;** ПЛИС (Field Programmable Gate Array, FPGA): Интегральная схема, которая может быть запрограммирована в условиях эксплуатации производителем системы контроля и управления. Она включает в себя программируемые логические блоки (комбинаторные и последовательностные), программируемые схемы соединений между ними и программируемые блоки для входов и/или выходов. Ее функцию определяет проектировщик системы контроля и управления, а не поставщик интегральной схемы.

Примечание — Хотя ПЛИС по существу представляют собой цифровые устройства, некоторые из них могут иметь в своем составе аналоговые входы/выходы и аналогово-цифровые преобразователи. ПЛИС могут включать в себя такие высокотехнологичные цифровые функции, как аппаратные умножители, выделенная память и встроенные ядра процессоров.

3.6 **язык описания аппаратных средств;** HDL (Hardware Description Languages, HDL): Язык, используемый для формального описания функций и/или структуры электронного компонента для ведения документации, моделирования или синтеза.

Примечание — Наиболее широко используются такие языки, как VHDL (IEEE 1076) и Verilog (IEEE 1364).

[1)] Заменен на IAEA SSG-39 «Design of Instrumentation and Control Systems for Nuclear Power Plants».

[2)] Согласно п. 46 НП-001-15, отказы по общей причине — это отказы системы (элементов), возникающие вследствие одного отказа или ошибки персонала или внутреннего или внешнего воздействия (события), или иной причины.

3.7 **HDL-программируемое устройство;** HPD (HDL-Programmed Device, HPD): Интегральная схема, конфигурированная (для СКУ АС) с использованием языков описания аппаратных средств и смежных программных инструментов.

Примечания

1 Языки описания аппаратных средств и смежные инструменты (например, средства моделирования и синтеза) используются для реализации требований к надлежащей сборке предварительно разработанных микроэлектронных ресурсов.

2 При разработке HPD могут быть использованы предварительно разработанные блоки.

3 Как правило, HPD базируются на заготовках ПЛИС, ПЛУ или подобных микроэлектронных технологиях.

3.8 **модуль** (module): Одна из частей, входящих в состав проекта; модуль может быть подразделен на другие модули.

Примечание — Слово «модуль» является синонимом слова «блок»; термин «блок» часто используют при проектировании электронных средств. Термин «модуль» применен в МЭК 60880, и потому его необходимо использовать в настоящем стандарте, использующем ссылку на МЭК 60880.

3.9 **встроенный блок** (native block): Блок, представляющий собой существующий ресурс в интегральной схеме, например ИЛИ-элемент или более сложный блок, такой как умножитель или контроллер последовательной передачи. Путем программирования HPD встроенные блоки конфигурируют и соединяют для обеспечения требуемой функции.

3.10 **список связей** (netlist): Описание электронного компонента с точки зрения взаимосвязей между его конечными элементами (например, встроенными блоками).

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

Примечания

1 ПРБ поставляют в виде библиотек, макроэлементов или IP-ядер. Их используют при разработке HPD и включают в это устройство.

2 Прежде чем включить ПРБ в HPD, может потребоваться значительная работа, например: синтезирование электронной схемы из HDL-операторов, отображение условных компонентов этой схемы на структурах аппаратных средств физической интегральной схемы и трассировка соединений.

3.12 **предварительно разработанное программное обеспечение** (Pre-Developed Software, PDS): Программное обеспечение, которое уже существует, доступно как коммерческий или запатентованный продукт и предполагается для применения.

[МЭК 60880]

3.13 **программируемое логическое устройство;** ПЛУ (Programmable Logic Device, PLD): Интегральная схема, состоящая из логических элементов со схемой взаимосвязей, части которой программирует пользователь.

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

Примечания

1 Существуют разные виды ПЛУ, например ПЛУ с возможностью стирания или сложное ПЛУ (СПЛУ).

2 Различия между ПЛИС и ПЛУ определены нечетко, но термин «ПЛУ» обычно применяют к более простому устройству, чем ПЛИС.

3.14 **уровень регистровых передач** (Register Transfer Level, RTL): Синхронная параллельная модель электронной схемы, описывающая ее поведение с помощью сигналов, обрабатываемых согласно комбинаторной логике и передаваемых между регистрами тактовыми импульсами. RTL-модель обычно пишут на HDL или создают с помощью исходного кода HDL.

4 Обозначения и сокращения

В настоящем стандарте использованы следующие обозначения и сокращения:

DRC — проверка проектных норм;

ESL — уровень электронной системы;

HDL — язык описания аппаратных средств;

HPD — HDL-программируемое устройство;

IP — объект авторских прав;
I&C — контроль и управление;
PDS — предварительно разработанное программное обеспечение;
RAM — запоминающее устройство с произвольной выборкой;
RTL — уровень регистровых передач;
SEU — единичный сбой;
SRAM — статическая оперативная память;
STA — статический временной анализ;
VHDL — сверхбыстродействующая интегральная схема на HLD;
V&V — верификация и валидация;
ООП (CCF) — отказ по общей причине;
ПЛИС (FPGA) — программируемая логическая интегральная схема;
ПЛМ (PAL) — программируемая логическая матрица;
ПЛУ (PLD) — программируемое логическое устройство;
ПРБ (PDB) — предварительно разработанный блок;
СИС (ASIC) — специализированная интегральная схема;
СПЛУ (CPLD) — сложное программируемое логическое устройство.

5 Общие требования к проектам HPD

5.1 Общие положения

Настоящий раздел в первую очередь устанавливает место HPD в системе контроля и управления, описанной в МЭК 61513. Затем раздел описывает жизненный цикл разрабатываемого устройства, который способствует более структурированному подходу к проекту HPD.

В конечном счете раздел устанавливает требования к проектам HPD, соблюдение которых обеспечивает гарантию качества и управление конфигурацией. Поскольку эти задачи сходны с целями разработки программного обеспечения, требования определяют с учетом соответствующих разделов МЭК 60880, при необходимости дополняя их специфическими требованиями для HPD.

Как указано в разделе 1, область применения настоящего стандарта не включает разработку микроэлектронных технологий или заготовок интегральных схем. Поэтому выражения «разработка HPD», «жизненный цикл HPD», «проект HPD», «верификация HPD» относятся к тому, что составляет процесс проектирования СКУ, начиная от разработки этих технологий или заготовок интегральных схем до создания конкретной интегральной схемы, предназначенной для применения в СКУ.

5.2 Жизненный цикл

Процесс создания систем контроля и управления для использования на атомных электростанциях представлен в МЭК 61513, который вводит понятие жизненного цикла системы. Это способ, посредством которого может быть проконтролирован процесс разработки и который позволяет получить данные, подтверждающие корректную работу систем безопасности. Он включает в себя установку требований, но не предписывает, каким образом должен быть осуществлен проект при создании систем (см. рисунок 1).

Понятие жизненного цикла системы по МЭК 61513 дополнено положениями МЭК 60880 (для функций категории А) и МЭК 62138 (для функций категории В и С) для разработки программного обеспечения, а также положениями МЭК 60987 для разработки аппаратного обеспечения компьютерных систем. Требования настоящего стандарта применяют к разработке HPD в системах класса 1 как дополнение к требованиям МЭК 60987.

Примечание — В случае противоречивости требований требования настоящего стандарта превалируют над требованиями МЭК 60987 в отношении HPD класса 1.

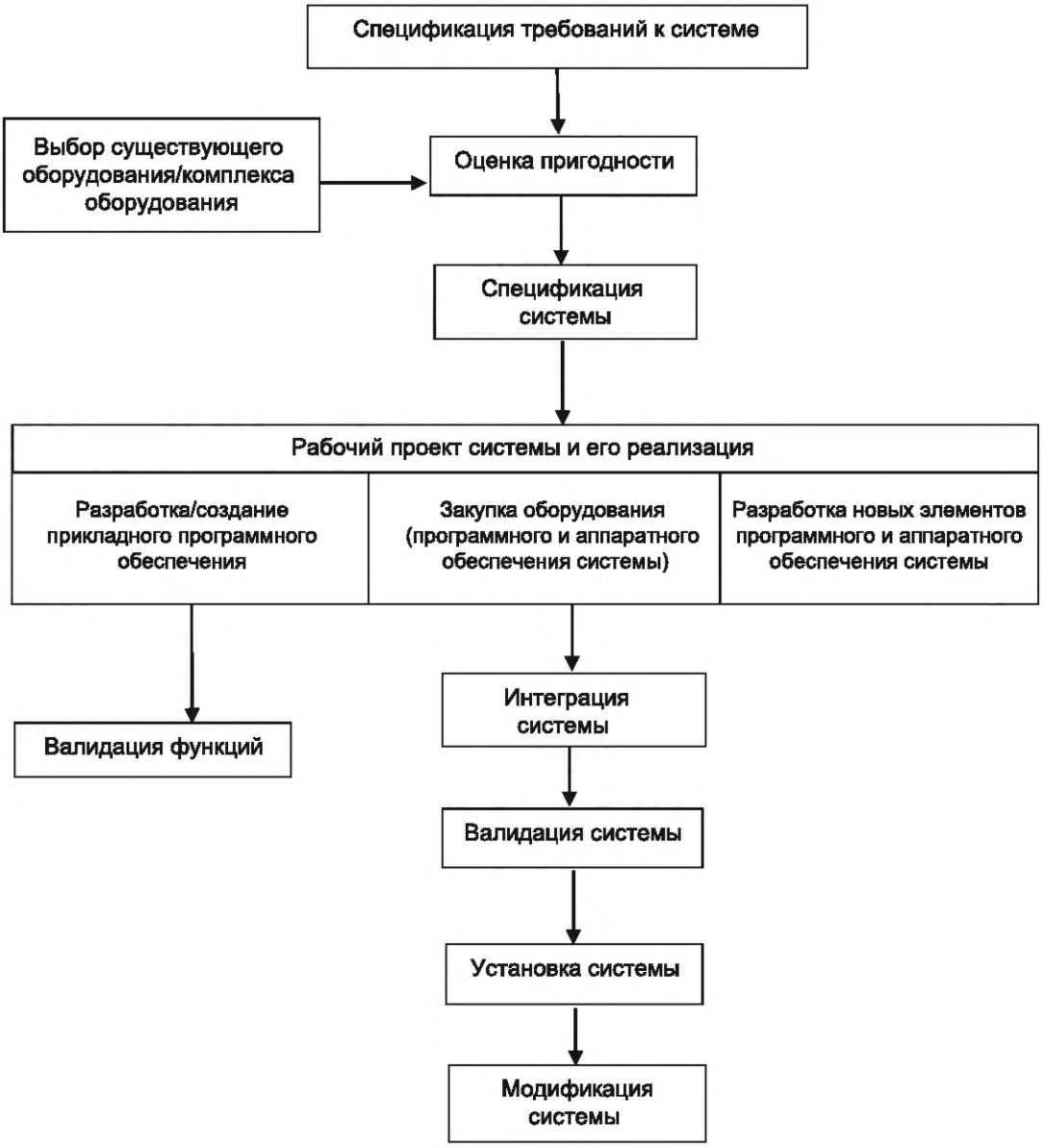

Рисунок 1 — Жизненный цикл системы (по МЭК 61513, для справки)

HPD разрабатывают с помощью компьютерных инструментов, что позволяет построить разработку в соответствии с жизненным циклом, включающим в себя действия по установлению требований, проектирование и реализацию, интеграцию и валидацию, а также верификацию и тестирование.

Этапы проектирования и реализации системы в соответствии с МЭК 61513, показанные на рисунке 1, особенно «Закупка оборудования (программного и аппаратного обеспечения системы)» и «Разработка новых элементов программного и аппаратного обеспечения системы», являются существенными этапами жизненного цикла системы в соответствии с МЭК 61513. Эти этапы представлены на рисунке 2, чтобы более подробно показать процесс от составления спецификации требований до валидации системных компонентов, которыми являются HPD.

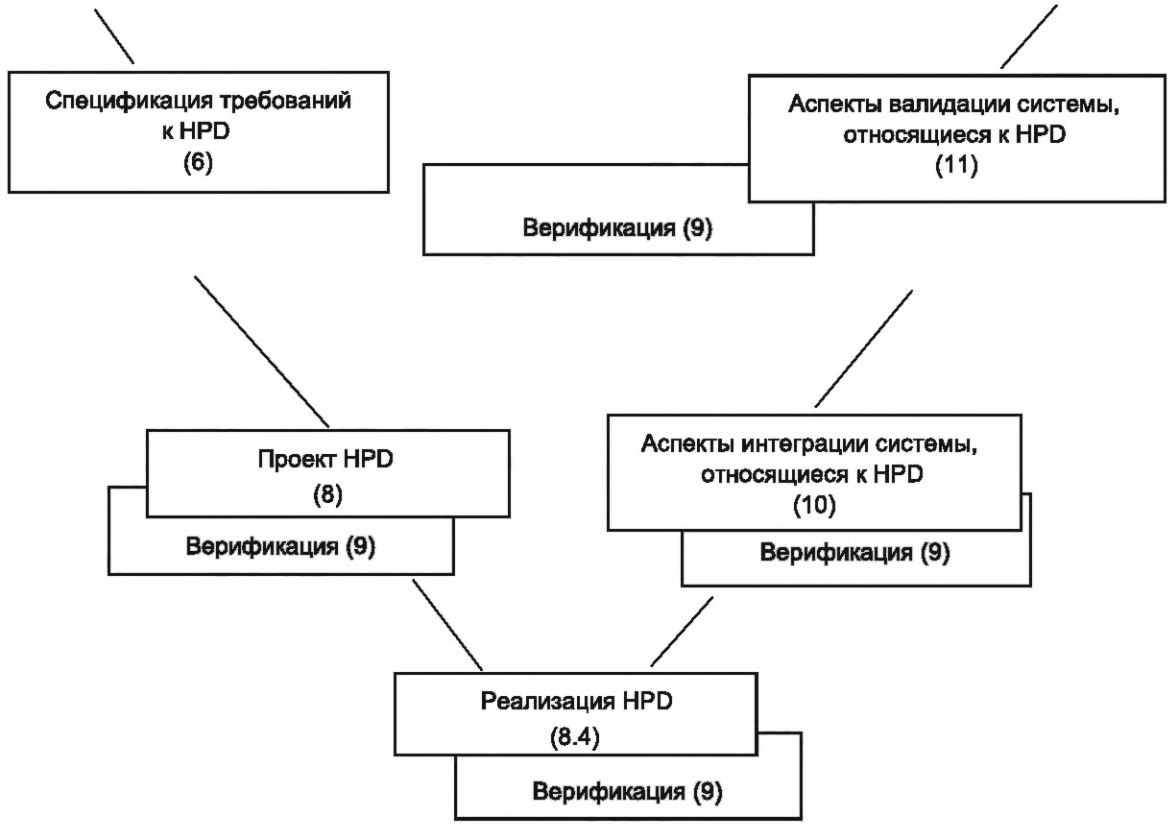

Рисунок 2 — Жизненный цикл разработки HPD

Разработчики, как правило, используют предварительно разработанные элементы, например заготовки программируемых интегральных схем или ПРБ для построения интегральных схем, приспособленных для нужд конкретного проекта. Мероприятия по выбору предварительно разработанных элементов приведены в разделе 7. Их можно проводить параллельно с первыми этапами жизненного цикла разработки, представленными на рисунке 2, при условии, что все взаимозависимости установлены и документально зафиксированы.

Жизненный цикл, представленный на рисунке 2, показывает жизненный цикл разработки одного HPD, которая может быть осуществлена параллельно с разработкой других компонентов (программного или аппаратного обеспечения) системы, как представлено на рисунке 1, но при этом все элементы должны быть одновременно подготовлены к этапам интеграции и валидации жизненного цикла системы.

Предложенный подход к разработке основан на традиционной модели V-образного цикла, поскольку такой подход отражен в других стандартах и рекомендован в нормах по безопасности МАГАТЭ NS-G-1.3, но следует предусмотреть необходимые корректировки, понимая, что некоторые этапы разработки могут выполняться имеющимися инструментами автоматически и этапы разработки могут быть повторяющимися.

Часто отсутствует четкое разделение и легко определяемая граница между интеграцией определенного компонента и интеграцией системы. Поэтому в настоящем стандарте интеграция HPD рассмотрена как часть интеграции системы. Аналогично валидацию HPD рассматривают как часть валидации системы.

В зависимости от функции, для выполнения которой предназначено HPD, на этапе интеграции могут быть рассмотрены системы или подсистемы:

1) начиная от системы контроля и управления, когда HPD реализует логику функции безопасности;

2) до электронной платы или монтажного шкафа, если HPD реализует функцию (внутреннюю по отношению к плате или шкафу), которая неспособна влиять на выходные сигналы какой-либо функции безопасности других элементов системы, что подтверждено надлежащим анализом.

Наиболее ответственной с точки зрения безопасности является ситуация, когда HPD непосредственно реализует логику функции безопасности.

Процесс разработки HPD предусматривает следующие мероприятия:

a) управление проектом (5.3);

b) обеспечение качества и контроль качества (5.4);

c) управление конфигурацией (5.5);

d) верификация[1)] (раздел 9).

Осуществляют также другие действия, включая выбор инструментов для поддержки разработки (раздел 15), подготовку документации (приложение А) и внесение изменений (раздел 12).

5.3 Управление проектированием HPD

5.3.1 Общие положения

5.3.1.1 Каждое HPD следует разрабатывать в рамках специально предназначенного для этого проекта HPD.

5.3.1.2 Проект HPD должен соответствовать требованиям 5.4 МЭК 60880:2006 (с заменой термина «программное обеспечение» термином «HPD»).

Примечания

1 Стандартный список документов, необходимых на протяжении всего жизненного цикла, приведен в приложении А.

2 Задокументированные входные данные, указанные в 5.4.6 МЭК 60880:2006, включают в себя параметры для автоматизированных действий программных инструментов (например, оптимизировать синхронизацию, оптимизировать плотность и т. п.).

5.3.1.3 Процесс разработки может быть итеративным; следующий этап может быть начат до того, как завершен предыдущий этап. В то же время, этап может быть закончен только в случае, если завершены предыдущие этапы и если его выходные данные согласуются с входными данными, предоставленными предыдущими действиями.

5.3.1.4 Этапы проектирования HPD должны включать в себя разработку спецификации требований, проектирование и реализацию HPD.

5.3.2 Дополнительные требования

5.3.2.1 Выбор предварительно разработанных элементов, используемых в проекте, следует осуществлять в соответствии с требованиями раздела 7.

5.3.2.2 Должны быть определены критерии перехода от одного этапа к другому.

5.3.2.3 Критерии завершения этапа должны иметь методологическое и техническое обоснование с достаточным уровнем детализации, предполагающим подробный анализ выходных данных этапа.

5.3.2.4 Документация (см. 5.4.11 в МЭК 60880:2006) должна содержать описание функций, выполняемых HPD, и его интерфейс.

5.4 План обеспечения качества HPD

Необходимо разработать план обеспечения качества HPD, который должен исходить из требований 5.5 МЭК 60880:2006 (с заменой термина «программное обеспечение» термином «HPD»).

Примечание — В этом контексте термин «язык» означает «компьютерный язык».

5.5 Управление конфигурацией

5.5.1 Управление конфигурацией HPD выполняют в соответствии с требованиями, изложенными в 5.6 МЭК 60880:2006 (с заменой термина «программное обеспечение» термином «HPD»).

Примечание — В соответствии с требованиями 5.6.6 МЭК 60880:2006 необходимо разделять документацию и компьютерные файлы, используемые или созданные при проектировании HPD.

5.5.2 Управление конфигурацией предусматривает фиксирование:

a) документации модулей (блоков), разработанных в рамках проекта, и ПРБ;

b) отличительной маркировки интегральных схем;

[1)] Согласно разделу 6 НП-026-16 верификация — это подтверждение на основе представления объективных свидетельств того, что результат деятельности на стадии жизненного цикла управляющей системы АС, важной для безопасности, получен с соблюдением требований, предъявляемых к этой системе на данной стадии жизненного цикла системы.

c) компьютерных файлов, используемых для моделирования, верификации и производства;

d) параметров, используемых для автоматизированных действий программных инструментов (см. раздел 15), например «оптимизация синхронизации, оптимизация плотности», при размещении компонентов и трассировке соединений;

e) идентификации версий всех программных инструментов (см. раздел 15), в том числе любых патчей к программному обеспечению, а также библиотек общего назначения и технологических библиотек.

6 Спецификация требований к HPD

6.1 Общие положения

6.1.1 Спецификация требований должна содержать требования к HPD в виде самих требований или в виде ссылок на набор требований, заданных на уровне системы или подсистемы (т. е. должно быть реализовано функциональное поведение).

6.1.2 Спецификация требований должна быть понятна для всех участников, включая инженеров аппаратного обеспечения и специалистов, упомянутых в 6.6.

6.1.3 Требования, входящие в спецификацию, должны быть недвусмысленны, верифицируемы и реально выполнимы, в том числе с точки зрения времени.

6.1.4 Если HPD выполняют функции безопасности, спецификация требований к ним должна быть составлена на основании требований к СКУ, осуществляющей эту функцию безопасности, и должна входить в спецификацию подсистемы, использующей HPD.

6.1.5 Спецификация требований должна предписывать, что следует делать, а не как следует это делать.

6.1.6 Для составления спецификации требований следует определить и внедрить задокументированную, официальную и контролируемую процедуру.

6.1.7 Спецификация требований должна быть составлена так, чтобы ее можно было проверить на соответствие спецификации требований к СКУ. Если HPD предназначено для использования подсистемой СКУ, также следует обеспечить возможность его проверки на соответствие спецификациям требований проекта системы.

6.1.8 Спецификация требований в отношении реализуемых функций должна учитывать все условия эксплуатации вплоть до уровня HPD, влияющего на выполнение данных функций.

6.1.9 Требования к интерфейсу с другими системами или компонентами следует рассматривать в соответствии с МЭК 61513.

6.1.10 Требования к интерфейсу с другими системами или компонентами должны быть задокументированы.

6.1.11 Нижеуказанные требования к интерфейсу должны быть документально зафиксированы, если они не входят в состав требований к HPD, а вытекают из решений, связанных с проектированием HPD:

a) электрические и временные характеристики (например, нагрузка на входе, время установки и удержания на входах, рабочая частота, разветвление на выходе, время прохождения сигнала от любого входа до соответствующих выходов),

b) профили сопрягаемого сигнала и источников электропитания,

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

6.2 Функциональные аспекты спецификации требований

Настоящий подраздел описывает содержание спецификации требований, непосредственно связанное с функциональными потребностями. Подразделы 6.3 и 6.4 посвящены дополнительным аспектам, которые необходимо включить в спецификацию требований.

Спецификация требований должна определять:

a) функции, реализуемые HPD;

b) различные режимы HPD и соответствующие условия перехода, в том числе включение электропитания и инициализацию;

c) интерфейсы HPD и взаимосвязи его с внешней средой (операторами и другими компонентами СКУ), в том числе роли, протоколы, типы, форматы данных, нумерацию битов, диапазоны и ограничения входов и выходов;

d) параметры, которые можно изменять вручную во время работы, и их роли;

e) производительность HPD, в частности время отклика;

f) что HPD не должно выполнять или чего следует избегать в соответствующих случаях;

g) любые допущения в отношении внешней среды HPD (например, электрические и временные характеристики входов-выходов, источники электропитания, заданные профили при включении питания, охлаждении).

6.3 Детерминированный подход

В спецификации требований должно быть указано, что функция HPD детерминирована проектом. Это означает, что любая конкретная последовательность входных данных, отвечающих за электрические и временные характеристики, всегда приводит к одинаковым результатам на выходе.

Примечание — Современные ПЛИС и другие интегральные схемы, входящие в область распространения настоящего стандарта, могут содержать аналоговые функциональные блоки (например аналогово-цифровой преобразователь), которые подвержены электронным помехам, погрешностям оцифровки и т. д. Различия в реакции этих аналоговых функциональных блоков по указанным причинам, а также их влияние на реакцию HPD не являются нарушениями в детерминированном проекте.

6.4 Выявление дефектов и сохранение работоспособности при наличии дефектов

К вопросам надежности по отношению к случайным отказам и климатическим условиям применимы требования по 5.3 и 5.4 МЭК 60987. К этим факторам относятся дефекты, обусловленные единичными сбоями (SEU) и альфа-нейтронным излучением в соответствующих случаях.

Защитное проектирование обычно основывают на сочетании нескольких технических решений (например, резервирование, принятие решений голосованием, паритетный контроль и циклический контроль резерва, сторожевой таймер, контроль диапазонов, проверка достоверности).

6.4.1 В спецификации требований устанавливают требования к защитному проектированию, направленному на выявление дефектов и сохранение работоспособности при наличии дефектов.

6.4.2 Польза от применения мер защитного проектирования должна компенсировать привносимую ими дополнительную сложность проекта. Основная задача заключается в том, чтобы на этапе проектирования и реализации учитывать возможность тестирования HPD, используя внутренние и внешние средства для максимально полного обнаружения дефектов.

6.4.3 Спецификация требований должна содержать описание мер, предпринимаемых для обнаружения неправильной работы HPD, учитывая при этом меры, уже предпринятые на уровне системы или подсистемы.

6.4.4 Указанные меры состоят в том, что HPD должно выдавать на выходе дополнительные данные либо для использования их внешним устройством, например сторожевым таймером, либо для обеспечения необходимого объема контроля, выполняемого внешним тестовым устройством.

6.4.5 Защитное проектирование должно обеспечивать обнаружение ошибочного поведения (например искажение данных, отклонение от определенного алгоритма обработки данных или отклонение от определенных рабочих условий), неправильной передачи данных между устройствами обработки данных, непреднамеренной модификации памяти или данных конфигурации.

6.4.6 Защитное проектирование не должно оказывать неблагоприятное влияние на функции СКУ и на возможность устройства HPD соответствовать требованиям быстродействия.

6.4.7 Спецификация требований должна содержать описание предполагаемых логических и временных характеристик (например значений выходных данных или конкретной выдаваемой информации) при выявлении дефектов.

6.4.8 Поведение, обусловленное такими характеристиками, должно соответствовать поведению системы, предусмотренному спецификацией на систему, и требованиям к проектированию системы согласно МЭК 61513.

6.4.9 В спецификации требований должен быть указан и обоснован запланированный уровень обнаружения дефектов, который должен быть достигнут с целью защитного проектирования.

6.5 Определение требований с использованием инструментов на уровне электронной системы

6.5.1 Общие положения

Настоящий стандарт не устанавливает специальный метод определения требований к HPD. Если эти требования определяют с использованием инструментов уровня электронной системы (ESL) (см. В.1), то к этим инструментам и их использованию применяют требования по 6.5.2 и 6.5.3.

При использовании инструментов ESL, когда язык спецификации требований аналогичен языкам реализации, следование требованиям по 6.1.5 может быть менее осуществимо [разделение того, что должно быть сделано (требование), и того, как это должно быть сделано (проект)]. Для того чтобы следование этим требованиям стало приемлемым, могут понадобиться некоторые условия, например комментарии, уточняющие входные и выходные данные и алгоритмы.

6.5.2 Требования к представлению инструментов, используемых на уровне электронных систем

6.5.2.1 При определении требований к HPD с использованием инструмента ESL:

a) этот инструмент должен предлагать наглядное представление со строгой семантикой (стандартизация структуры и способа представления, модульный подход, содержательные комментарии);

b) представление, используемое в этом инструменте ESL, должно быть понятно всем участникам;

c) если инструмент предлагает гибкие механизмы перераспределения функций и операторов, то реальные характеристики каждого элемента должны быть доступны всем участникам, в том числе инженерам по разработке аппаратного обеспечения и специалистам, упомянутым в 6.6.

6.5.2.2 Языки, используемые на уровне электронных систем, должны позволять учитывать архитектуру системы, например разрешать назначение функций компонентам и поддерживать проектные решения по сохранению работоспособности.

6.5.3 Интерфейс с проектными инструментами

Семантика языков, используемых для выражения спецификации требований на уровне электронных систем, может отличаться от семантики языков описания аппаратных средств, используемых при проектировании. Расхождения могут иметь место, например, при интерпретации параллельно обрабатываемых данных, управлении переполнениями или кодировании типов и конечных автоматов.

a) Если семантика языка для выражения спецификации требований на уровне электронных систем отличается от семантики других языков, используемых в проекте, то их расхождения должны быть идентифицированы для каждого элемента, включенного в спецификацию требований. Каждый случай расхождения в спецификации требований должен быть задокументирован.

b) Общий перечень расхождений между примененными языками представляет собой полезный справочный материал, но не является достаточным для внесения полной ясности в спецификацию требований.

6.6 Анализ и пересмотр требований

6.6.1 Для обнаружения потенциальных несоответствий, пропусков и двусмысленностей проводят критический анализ требований, результаты которого документируют.

6.6.2 Предметом такого анализа должны быть функциональные требования и все другие виды требований, в том числе касающиеся нештатного поведения, например поступления непредвиденных входных параметров или нарушения последовательности.

6.6.3 Спецификацию требований следует пересматривать с целью проверки их полноты и согласованности.

6.6.4 Для анализа функций безопасности, реализуемых HPD, в процессе пересмотра должны принимать участие специалисты по контролю и управлению, обработке данных, а также специалисты по подсистемам и компонентам (в том числе по их программному обеспечению), сопряженным с HPD.

7 Процесс приемки программируемых интегральных схем, встроенных блоков и предварительно разработанных блоков

7.1 Общие положения

При разработке HPD необходимо отбирать и оценивать предварительно разработанные элементы, например заготовки интегральных схем (в том числе их встроенные блоки) или предварительно разработанные блоки, входящие в состав окончательного варианта HPD.

Поскольку эти предварительно разработанные элементы (или компоненты) могут включать ненужные для HPD функции, может быть рекомендована разработка и соблюдение специальных правил использования элементов, чтобы ограничить их применение только тем, что необходимо и безопасно.

7.2 Спецификация требований к компонентам

7.2.1 Общие положения

Требования, предъявляемые к предварительно разработанным блокам (или компонентам), вытекают из начальных действий по проектированию HPD. Например, требования к HPD могут включать наличие специального полосового фильтра, который может быть внедрен проектировщиком с помощью ПРБ, выполняющего быстрое преобразование Фурье.

Таким образом, спецификация требований к компоненту (в данном случае к ПРБ для быстрого преобразования Фурье, характеризуемому типом алгоритма, объемом выборки, методом прореживания, площадью кремниевого кристалла и т. д.) отличается от спецификации требований к HPD (в данном случае к полосовому фильтру, характеризуемому сопрягающей частотой, коэффициентом усиления, крутизной спада и т. д.).

7.2.1.1 В спецификации требований к компоненту должны быть документально зафиксированы требования, применяемые к каждому предварительно разработанному элементу: заготовке интегральной схемы, микроэлектронным ресурсам (рассматриваемым как встроенные блоки), сопутствующим инструментам в соответствующих случаях или к ПРБ.

7.2.1.2 Спецификация требований к компоненту должна представлять все требования либо в виде отдельного документа, либо в виде ссылок на набор требований, указанных на уровне системы или подсистемы (например, функциональное поведение, которое должно быть реализовано).

7.2.1.3 Будучи основой для выбора и использования предварительно разработанного элемента, спецификация требований к компоненту должна быть понятна всем участникам, в том числе разработчикам соответствующего аппаратного и программного обеспечения, лицам, осуществляющим контроль, проверяющим и представителям регулирующих органов.

7.2.1.4 Спецификация требований к компоненту должна быть недвусмысленной, верифицируемой и реально выполнимой, в том числе с точки зрения времени.

7.2.1.5 Спецификация требований к компоненту должна быть такой, чтобы система контроля и управления, использующая этот компонент, соответствовала требованиям МЭК 61513.

7.2.2 Требования

Спецификация требований к компоненту должна устанавливать все необходимые характеристики включенного предварительно разработанного элемента, особенно характеристики, важные для выполнения требований, приведенных в 6.2.

Примечание — Типовые названия характеристик («функция») идентичны названиям, указанным в 6.2, но их содержание в большинстве случаев отличается, как сказано в 7.2.

7.2.3 Анализ и проверка требований

7.2.3.1 Для обнаружения возможных несоответствий, недостаточной полноты и двусмысленностей необходимо проводить критический анализ спецификации требований к компоненту, оформляя его документально.

7.2.3.2 Предметом такого анализа должны быть функциональные требования и все другие виды требований, в том числе требования, касающиеся нештатного поведения, например появления непредвиденных входных параметров или нарушения последовательности.

7.2.3.3 Спецификацию требований к компоненту в установленном порядке предъявляют к рассмотрению специалистам всех соответствующих областей с целью проверки полноты и согласованности требований.

7.3 Правила использования

7.3.1 Если в предварительно разработанном элементе предусмотрены функции или рабочие режимы, реализация которых не требуется при работе HPD, то должны быть установлены правила, запрещающие использование таких функций и режимов.

Использование функций или режимов, реализация которых необходима при работе HPD, может быть ограничено правилами в целях улучшения проектных параметров, таких как безопасность или пригодность к испытаниям.

7.3.2 Если правила использования установлены:

a) они должны быть документально зафиксированы;

b) план обеспечения качества должен служить подтверждением того, что выполнение этих правил проверяется в ходе реализации проекта.

7.4 Выбор

7.4.1 Общие положения

7.4.1.1 Документально оформленный анализ каждого предварительно разработанного элемента, используемого в HPD, должен подтверждать, что этот элемент отвечает требованиям, указанным в спецификации требований к компоненту, который он представляет или частью которого он является, возможно в соответствии с правилами использования и модификаций (см. 7.6).

7.4.1.2 Пользовательская документация по безопасности должна содержать подробные указания о том, как разработчикам следует использовать предварительно разработанный элемент в соответствии с его спецификацией и проектными характеристиками.

7.4.2 Проверка документации

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

7.4.2.1 Такая проверка должна быть выполнена на основании документации предварительно разработанного элемента, в том числе документации по его разработке и верификации.

7.4.2.2 Документация должна содержать достаточно сведений, подтверждающих соответствие предварительно разработанного элемента функциональным, электротехническим и временным требованиям.

7.4.2.3 Анализ документации должен подтверждать, что функции и режимы предварительно разработанного элемента, не используемые при работе HPD, не препятствуют использованию необходимых функций и режимов.

7.4.3 Анализ опыта эксплуатации

Для компенсации некоторых недостатков документации, касающихся надежности или конструкции элемента, может быть привлечен опыт эксплуатации предварительно разработанного элемента. В случае привлечения опыта эксплуатации:

a) анализ опыта эксплуатации должен показать, что:

1) его объем адекватен требованиям надежности,

2) опыт приобретен в рабочих условиях, аналогичных тем, в которых будет использоваться предварительно разработанный элемент,

3) фактическое использование предварительно разработанного элемента прослежено настолько детально, как этого требует настоящий стандарт в отношении документации;

b) средства и процедуры, использованные для сбора данных об опыте эксплуатации, должны гарантировать, что любой отказ предварительно разработанного элемента, имевший место в анализируемой практике, зафиксирован настолько подробно, что путем технического анализа можно установить причину отказа, насколько это возможно;

c) анализ отказов, зафиксированных во время работы, должен подтверждать, что отказы не имеют воздействия на функции или безопасность HPD;

d) опыт эксплуатации и, если необходимо, дополнительные испытания должны подтверждать, что предварительно разработанный элемент соответствует предъявляемым к нему требованиям;

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

f) анализируемый опыт эксплуатации должен относиться к практике применения точно определенных вариантов предварительно разработанного элемента и оборудования, в котором он работает, если этот элемент является специфическим для этого оборудования;

g) опыт эксплуатации должен относиться к применению определенного варианта предварительно разработанного элемента или его части, используемых в HPD. В противном случае необходимо проанализировать различия в вариантах, чтобы подтвердить, что опыт эксплуатации подходит для заданного варианта.

7.4.4 Особые требования в отношении заготовок интегральных схем

7.4.4.1 Следует рассмотреть следующие аспекты:

a) анализ соответствия механизмов программирования и компоновки схемы;

b) подтверждение того, что процесс программирования не имеет дефектов или что любой дефект при программировании обнаружен и корректно устранен;

c) подтверждение того, что интегральная схема сохраняет свою запрограммированную конфигурацию на необходимый период;

d) анализ возможности отказов, связанных с дополнительными внутренними и внешними механизмами или переходными помехами по цепи питания, и обоснование применения в соответствии с требованиями надежности.

7.4.4.2 Подробный анализ должен подтверждать, что:

a) интегральная схема сможет соответствовать требованиям, указанным в спецификации требований к компоненту;

b) сопутствующие инструменты:

- соответствуют положениям раздела 15,
- обеспечивают возможность всех верификаций, предусмотренных разделами 8 и 9 (например, статического временного анализа).

7.4.4.3 Данные, необходимые для расчета частоты отказов (имея в виду случайные физические отказы), должны быть доступны и основаны на достаточном опыте эксплуатации.

7.4.4.4 Специалисты, занимающиеся разработкой и внедрением HPD, должны обладать необходимыми знаниями в следующих областях:

a) заготовки интегральных схем, в том числе особенности программирования, конфигурирование и тестовые режимы, работа с протоколами, контакты и регистрирующие устройства, специфика электрических и логических систем;

b) сопутствующие инструменты, встроенные блоки и ПРБ. При этом они должны уметь прогнозировать, понимать и, при необходимости, управлять выбором, сделанным с помощью этих инструментов во время синтеза, размещения и трассировки.

7.5 Обоснование приемки

7.5.1 Путем формального пересмотра следует проверять анализ предварительно разработанных элементов, включая правила использования и действия, предпринятые для обеспечения соответствия установленным требованиям каждого физического элемента, используемого в промышленной эксплуатации, чтобы решить, пригоден или не пригоден предварительно разработанный элемент для использования в HPD.

7.5.2 Если предварительно разработанный элемент признан пригодным, то любое действие и правило использования, прошедшее анализ, считают применимым на протяжении всего жизненного цикла HPD.

7.5.3 В состав группы специалистов, осуществляющих пересмотр, необходимо включать экспертов, обладающих профессиональными знаниями в соответствующих областях (например, технология аппаратных средств, программное обеспечение), и инженеров из групп, отвечающих за компоненты, сопрягаемые с предварительно разработанным элементом.

7.6 Внесение изменений для приемки

7.6.1 Если для приемки необходимо внести изменения в предварительно разработанный элемент, то эти изменения должны быть определены, разработаны, реализованы и верифицированы до начала пересмотра.

7.6.2 Эти изменения должны быть выполнены и задокументированы в соответствии с требованиями настоящего стандарта, касающимися структуры и исполнения проекта, качества, спецификации требований, проектирования, реализации и верификации.

7.7 Внесение изменений после приемки

Процедуру приемки, в том числе формальный пересмотр, необходимо выполнять каждый раз после внесения каких-либо изменений в предварительно разработанный элемент, включая изменения, касающиеся проекта или микроэлектроники.

7.8 Документация для приемки

Работа с документацией по приемке предварительно разработанного элемента является частью управления конфигурацией.

7.8.1 В состав документации должны входить следующие документы или ссылки на них:

a) спецификация требований к HPD;

b) все документы, составленные или использованные при анализе предварительно разработанного элемента;

c) все документы, оформленные в процессе внесения изменений в предварительно разработанный элемент;

d) отчет о пересмотре.

Документация должна включать в себя всю информацию, необходимую для корректного использования предварительно разработанного элемента, с указанием ограничений первоначальных требований спецификации, правил использования и модификаций.

8 Проектирование и реализация HPD

8.1 Общие положения

В настоящем разделе приведены требования и рекомендации, основанные на передовой практике проектирования и реализации, направленные на обеспечение соответствующих характеристик безопасности, таких как максимальная безотказность и возможность верификации.

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

8.2 Языки описания аппаратных средств (HDL) и сопутствующие инструменты

Несмотря на то что нельзя требовать использования конкретных языков и инструментов, в качестве общих основных правил применения языков и инструментов для проектирования и реализации HPD, предназначенных для систем класса 1, можно рассматривать следующие положения.

8.2.1 Для проектирования и реализации следует использовать языки описания аппаратных средств (HDL) и инструменты для моделирования, синтеза, размещения и трассировки.

Примечание — Надлежащий выбор и использование этих инструментов способствуют улучшению таких существенных параметров, как понятность описаний, управление электрическими и временными ограничениями, верификация, корректность критериев применимости, документация.

8.2.2 Даже если условие по 8.2.1 не выполнено, вся документация, анализ или верификация в соответствии с настоящим стандартом должны быть обеспечены.

8.2.3 Используемый язык должен:

a) следовать строгим (или четко определенным) правилам семантики и синтаксиса;

b) иметь четко и полноценно определенный и документально зафиксированный синтаксис;

c) соответствовать признанному стандарту (например, IEEE 1076 для VHLD или IEEE 1364 для языка Verilog).

8.2.4 Там, где это целесообразно, следует ограничить использование языка сферой безопасности, например сохраняя его применение только для реализации требуемых функций и возможности сочетания со стандартизованными библиотеками (избегая употребление начальных значений, явных задержек или деления).

8.2.5 Используемое средство моделирования должно выдавать результаты в строгом соответствии с задокументированной семантикой языка.

Средство моделирования должно соответствовать признанному стандарту (например, IEEE 1076 для VHLD или IEEE 1364 для языка Verilog).

8.2.6 За исключением случая, указанного в 8.2.7, для анализа, моделирования, синтеза, размещения и трассировки следует использовать только инструменты, соответствующие требованиям раздела 15. Если тестирование инструментов выполнено и оформлено документально поставщиком, то отсутствует необходимость его повторять.

8.2.7 Если используют инструмент, частично соответствующий требованиям раздела 15, то для подтверждения правильности, результатов, выдаваемых этим инструментом (например, список связей, выдаваемый инструментом моделирования), необходима дополнительная верификация результатов. Важным средством получения проекта, свободного от ошибок, являются инструменты проверки формальной эквивалентности.

8.3 Проектирование

8.3.1 Общие положения

Начиная со спецификации требований к HPD, первоначальной задачей проектирования является определение основных вариантов разбиения на модули (специализированные или предварительно разработанные), разработки защитного проекта, а также идентификация необходимого микроэлектронного оборудования (включая встроенные блоки) и ПРБ. Затем создают описание уровней регистровых передач (RTL), используя языки описания аппаратных средств. Приведенные ниже требования нацелены на создание понятного и верифицируемого проекта.

8.3.1.1 На стадии проектирования необходимо получить:

a) формализованное описание HPD, например на уровне регистровых передач, и

b) соответствующую документацию.

8.3.1.2 Коммуникационные каналы должны быть спроектированы в соответствии с требованиями к передаче данных, приведенными в 5.4.2.4 МЭК 61513.

8.3.1.3 Проект должен способствовать легкому проведению верификации.

8.3.1.4 Несоблюдение правил проектирования должно быть обосновано.

8.3.2 Защитное проектирование

8.3.2.1 Если выбранный встроенный блок или ПРБ (см. раздел 7) является ядром процессора, он должен соответствовать требованиям МЭК 60880, относящимся к самоконтролю.

8.3.2.2 Проект должен учитывать меры, предусмотренные в спецификации требований для выявления дефектов и формирования соответствующей информации в HPD.

8.3.2.3 При выявлении дефекта HPD должно реагировать в соответствии с определенными требованиями.

8.3.3 Структура

8.3.3.1 Принцип разработки проекта «сверху вниз» предпочтительнее принципа разработки «снизу вверх».

Примечание — Конечной целью проектирования являются элементы библиотеки. Рекомендуется использовать библиотеки, удовлетворяющие требованиям разделов 7 и 15, что соответствует принципу разработки «сверху вниз».

8.3.3.2 Структура проекта должна быть основана на разбиении на модули. Соответствующие модули могут содержаться в библиотеке.

8.3.3.3 Типовые модули должны содержаться в библиотеках.

8.3.3.4 Структура должна быть простой и понятной как в целом, так и в деталях.

8.3.3.5 Концептуальная модель архитектуры должна быть разработана на начальном этапе проектирования.

8.3.4 Язык и правила написания кода

8.3.4.1 Для того чтобы обеспечить устойчивый и надежный проект, следует применять апробированную методологию проектирования и общую положительную практику.

8.3.4.2 Для того чтобы сделать проект более понятным и снизить вероятность различий между моделируемым и синтезируемым поведением:

a) необходимо в соответствии с планом обеспечения качества установить ряд строгих правил проектирования, отражающих новейшие знания в части проектной безопасности и надежности;

b) соблюдение указанных правил проектирования необходимо обеспечивать соответствующими средствами (например, проводить анализ, применять необходимые инструменты и т. д.).

8.3.4.3 Ниже приведен перечень настоятельно рекомендуемых ограничений и методик проектирования. Однако указанный перечень не является всеобъемлющим и может меняться с изменением технологий. Тем не менее любое несоблюдение приведенных ниже правил необходимо обосновывать и учитывать при анализе отказов:

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

b) там, где это необходимо, следует использовать специализированные ресурсы или конструктивные особенности (например, заданные древовидные синхронизации импульсов и согласование каналов связи, шины электропитания, древовидные схемы сброса и т. д.);

c) правила написания кода должны относиться ко всем аспектам, в частности: к наименованию модулей и сигналов, использованию функций образования структур (программных пакетов, функций, процедур, проектных библиотек, отдельных объектов), организации вычислений по критическим путям, организации процессов, рекомендуемым конструкциям, запрещенным конструкциям;

d) в описании проекта следует запретить функции, использующие побочные эффекты (обоснование: данная функция может возвращать разные значения, если ее запрашивать несколько раз с одинаковыми параметрами. В связи с этим трудно проводить испытание и верификацию, поскольку нарушаются базовая концепция функции и, по сути дела, детерминизм).

Примечание — Указанная функция может также иметь такие побочные эффекты, как модификация объектов вне области их применения;

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 сравнениях, 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) присваивать начальные значения (инициализировать) сигналам и переменным следует не при их декларировании в описании на уровне регистровых передач (RTL), а при задействовании явно заданного механизма процесса, такого как сброс. (Обоснование: присвоение значений с применением 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 — Это правило не запрещает существование задержек на уровне системы или в требованиях к HPD. Это означает, что такие задержки не допускается реализовать командой «задержка» («delay») или «после» («after») на HDL, но можно, например, с помощью счетчиков или сдвиговых регистров;

h) в проектном описании следует запретить создание задержек посредством комбинаторных схем или в результате зависимости от распространения задержек по проводам. Если избежать такого решения нельзя, то необходимо выполнить статический временной анализ (STA), чтобы обосновать использование такой конструкции (обоснование: указанные задержки неустойчивы по таким параметрам, как температура, напряжение, а также могут изменяться от одной части к другой, или от одной зоны кристалла интегральной схемы к другой);

i) типы сигналов интерфейса HPD должны быть определены четко и однозначно, предпочтительно стандартным образом, независимо от инструментов или микроэлектронных технологий;

j) определения на уровне HDL не должны допускать разные интерпретации во избежание вариаций в процессе компиляции при различных условиях. Например, входные/выходные сигналы HPD следует явно назначать на известные контактные выводы схемы.

Примечания

1 Требования настоящего подраздела неприменимы к проектированию библиотечных компонентов, которые выстраивают для реализации в различных местах будущих конструкций с различными распределениями ввода/вывода.

2 Для разработки кода HDL, который можно передавать от одной единицы оборудования к другой, необходимо определить расположение контактных выводов в файле ограничений, а не в коде HDL. Помочь в этом могут языковые функции, такие как шаблоны в языке VHDL-2008.

8.3.5 Синхронное и асинхронное проектирование

Синхронное проектирование заключается в одновременном принудительном изменении состояния внутренних регистров и выходных сигналов только в моменты времени, задаваемые генератором тактовых импульсов. Это помогает создать модульную структуру проекта и облегчить его понимание, минимизирует вероятность некорректного поведения из-за сбоев и способствует наиболее эффективному использованию инструментов синтеза и верификации.

8.3.5.1 Для создания надежного, полноценного и четко структурированного проекта необходимо:

a) использовать строго синхронизированную архитектуру;

b) обосновывать факты несоответствия требованиям.

8.3.5.2 Проект должен обеспечивать синхронизацию сигналов в асинхронных интерфейсах.

8.3.5.3 При использовании асинхронной архитектуры документально зафиксированный анализ всех контуров сети должен подтвердить соответствие выходных сигналов спецификации требований (см. раздел 6) и отсутствие нежелательных сбоев или метастабильных состояний.

8.3.5.4 Поведение HPD не должно зависеть от фактических значений внутренних задержек распространения сигнала по проводам и через шлюзы.

8.3.6 Управление режимом электропитания

8.3.6.1 Внутренние электрические и временные характеристики заготовки интегральной схемы во время включения электропитания/запуска, выключения электропитания и внезапной потери электропитания должны быть известны и учтены в ходе проектирования.

8.3.6.2 Информацию о поведении каждого контактного штыря (например, входного или выходного типа, импеданса) 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 опираться на допущение того, что они ведут себя в соответствии с запрограммированным режимом (например, относительно функций, направления и импеданса каждого контактного штыря) при включении электропитания/запуске, выключении электропитания и внезапной потере электропитания, даже в случае однократно программируемых устройств.

8.3.6.4 Соединение входных контактных штырей с источником напряжения или с землей следует выполнять согласно указаниям поставщика по применению, чтобы избежать возможных пиков тока при включении электропитания/запуске, выключении электропитания и внезапной потере электропитания.

8.3.6.5 Если распределение электропитания не установлено поставщиком компонентов, необходимо при проектировании уделить этому особое внимание, чтобы избежать недетерминированных дефектов из-за таких проблем, как подъемы напряжения, обусловленные пиками тока на фронтах тактового сигнала.

8.3.7 Инициализация

8.3.7.1 Схема должна иметь 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 цифровую природу, соответствовал требованиям к заготовке интегральной схемы, таким как время нарастания, время спада импульса или монотонность.

8.3.7.3 Подтверждение этого сигнала должно иметь запланированный эффект, даже когда часы не работают и действий по синхронизации не происходит.

8.3.7.4 Отмену подтверждения этого сигнала необходимо выполнять таким образом, чтобы указанное начальное состояние всех выходных сигналов, регистров и конечных автоматов сохранялось, когда часы работают, т. е. пока идет синхронизация.

8.3.8 Нефункциональные конфигурации

8.3.8.1 Необходимо проанализировать и сконфигурировать специальные контактные штыри и регистры, которые позволяют подключать HPD в специальные схемы (такие, как испытание, диагностика, отладка программы или программирование) и которые не определены спецификацией требований к HPD, чтобы исключить любое неблагоприятное воздействие на их функции.

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

8.3.8.3 Управление контактными штырями и регистрами конфигурации HPD должно быть оформлено документально.

8.3.9 Контролепригодность

8.3.9.1 Необходимо, чтобы каждая функция, реализуемая в HPD, была контролепригодной (с возможностью выявления отказов) с использованием таких методов, как самоконтроль, периодические испытания или наблюдение за ее участием в выполнении функции более высокого уровня, которая подвергается отдельному самоконтролю или периодическим испытаниям.

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

8.3.9.3 Следует определить реальный уровень обнаружения дефектов (см. 6.4.9) и периодических испытаний, который должен соответствовать спецификации требований к HPD.

8.3.9.4 Необходимо минимизировать последствия дефектов, например, путем распознавания таких достигнутых состояний, которые обычно недостижимы, и осуществления в таких случаях предопределенного действия.

8.3.10 Проектная документация

8.3.10.1 По окончании этапа проектирования необходимо подготовить соответствующую документацию.

8.3.10.2 В документации следует описать и обосновать адекватность проектных решений с точки зрения соответствия спецификации требований к HPD.

8.3.10.3 Проектная документация должна быть достаточно полной, чтобы реализацию можно было осуществить без дальнейших разъяснений.

8.3.10.4 В документации необходимо описать следующие проектные решения:

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

b) потоки команд 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 указать вариант, фактически используемый для каждого экземпляра каждого компонента библиотеки, чтобы избежать неоднозначностей в тех случаях, когда существуют варианты с различным быстродействием или электрическими характеристиками.

8.3.10.6 В проектную документацию должны быть включены все параметры, необходимые для однозначного конфигурирования и использования всех встроенных блоков и ПРБ.

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 на уровне регистровых передач (RTL), в ходе реализации синтезируют описание HPD на уровне логических элементов (список связей). Затем выполняют размещение и трассировку, завершая физическим описанием HPD (программирующий файл или битовый поток), необходимым для изготовления устройства.

8.4.2 Результаты

8.4.2.1 В ходе реализации формируют в систематизированном виде всю информацию, необходимую для изготовления HPD и для проверки того, что каждая изготовленная часть соответствует проекту.

8.4.2.2 В ходе реализации в дополнение к описанию RTL необходимо подготовить информацию о синхронизации («обратное аннотирование»), чтобы точно смоделировать временное поведение с учетом всех задержек, связанных с логическими элементами и проводными соединениями.

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 руководит операциями синтеза, размещения и трассировки с помощью параметров и директив, которые конкретизируют ограничения, такие как необходимая рабочая частота, синхронизирующие соотношения между сигналами или коэффициент разветвления по выходу. Для вы-

полнения этих ограничений (передаваемых инструментам в файлах ограничений) инструменты могут модифицировать размещение, отдавая предпочтение данному тракту распространения сигнала за счет других, дублируя одну логическую схему для снижения нагрузки на каждый экземпляр, увеличивая таким образом их быстродействие и т. д.

Ошибки или упущения в параметрах и файлах ограничений могут привести к труднодиагностируемым непредвиденным дефектам, которые часто нельзя обнаружить во время моделирования и которые чувствительны к нормальным отклонениям в работе микроэлектроники.

8.4.3.1 Файлы параметров и ограничений следует строить согласно процессу, который может быть проконтролирован.

8.4.3.2 Полнота и правильность файлов параметров и ограничений должна быть подтверждена группой, проводящей верификацию (см. раздел 9).

8.4.3.3 Файлы параметров и ограничений должны быть документально оформлены и помещены под управление конфигурацией.

8.4.4 Анализ после трассировки

8.4.4.1 Анализ, проводимый после трассировки, должен подтвердить соответствие проекта и его реализации технологическим нормам, установленным поставщиками инструментов проектирования и реализации, и используемой микроэлектронной технологии.

8.4.4.2 Анализ, проводимый после трассировки или процессов моделирования (с учетом информации о пост-трассировочной синхронизации или обратного аннотирования), должен подтвердить пошаговую эквивалентность пост-трассировочного описания и описания RTL для самых быстрых и самых медленных процессов, включая инициализацию, используя для этого процедуру, состоящую, например, из следующих двух этапов:

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

b) подтверждение того, что описание после трассировки согласуется с ограничениями синхронизации.

8.4.4.3 При моделировании после трассировки допускается использовать только часть случаев моделирования на испытательном стенде, применяемых в моделировании RTL (см. 9.5). Необходимо обосновать, что данная часть позволяет обеспечить потребность в подтверждении эквивалентности. Альтернативный или дополнительный метод моделирования после трассировки заключается в использовании инструмента, который проверяет математическую эквивалентность уровня регистровых передач (RTL) и уровня физического описания. Если принимают данный подход, то качество и пригодность инструмента, используемого для выполнения указанной проверки, необходимо оценить перед его применением (см. раздел 15).

8.4.4.4 Синхронизации, проведенные после трассировки, следует подвергнуть анализу.

8.4.4.5 Охват каждой функции самоконтролем необходимо проанализировать с учетом требования к уровню обнаружения дефектов (см. 6.4.9), принимая во внимание возможное влияние инструментов на фактическую сетевую топологию.

8.4.4.6 Такой анализ должен быть достаточно подробным и задокументированным, что позволит провести дальнейшую техническую оценку лицами, не занятыми в проектировании и реализации.

8.4.4.7 Некоторые виды такого анализа можно выполнить по выбору или автоматически с помощью программных инструментов. В таком случае не требуется выполнять анализ повторно, но при этом:

a) необходимо подтвердить, что анализ, выполненный с использованием инструментов, обеспечивают требуемое покрытие и корректность;

b) отчеты об анализе (включая план анализа и его результаты), проведенном с использованием инструментов, должны быть включены в состав документации.

8.4.4.8 Если при анализе обнаружены несоответствия, признанные приемлемыми, то:

a) приемлемость должна быть обоснована и документально оформлена;

b) все документы, имеющие к этому отношение, должны быть соответствующим образом изменены;

c) план обеспечения качества должен гарантировать, что любое влияние на другие системы или компоненты документально фиксируется и учитывается лицами, ответственными за эти системы и компоненты.

8.4.5 Избыточность, обеспечиваемая или ликвидируемая при использовании инструментов

8.4.5.1 Следует проанализировать повторения логических элементов, выполняемые инструментами для соблюдения соответствия временным характеристикам и технологическим ограничениям.

8.4.5.2 Необходимо подтвердить, что дополнительные состояния, вводимые в результате этих повторений, приемлемы с точки зрения функциональных требований и требований безопасности. Считается, что повторения логических элементов выполняются многими инструментами синтеза, но, как правило, ими же адекватно контролируются. Однако следует обратить внимание, что повторение логических элементов может вызвать проблемы в случае проведения аналогичной проверки эквивалентности для обоснования RTL и реализации логического элемента.

8.4.5.3 Поскольку повторение вводит новые состояния, их необходимо проанализировать и показать, что они не влияют на безопасное поведение проектируемой системы.

8.4.5.4 С другой стороны, необходимо подтвердить, что выполняемая инструментами логическая оптимизация не удалила механизмы обнаружения дефектов и обеспечения отказоустойчивости, такие как избыточность или обработка случаев, недостижимых в нормальных условиях.

8.4.6 Конечные автоматы

8.4.6.1 Необходимо проанализировать надежность 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 — Тупиковым состоянием называется состояние, из которого конечный автомат не может перейти ни в какое другое состояние.

8.4.6.3 При анализе отказов необходимо учитывать возможные дополнительные состояния, вводимые некоторыми методами кодирования (например, методом прямого кодирования).

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 состояние «ложь». Таким образом, действительны только комбинации ровно с одним триггером, установленным в состояние «истина». В случае отказа несколько триггеров могут быть одновременно установлены в состояние «истина», что будет соответствовать дополнительным, неопределенным состояниям.

8.4.7 Статический временной анализ

8.4.7.1 Необходимо выполнить и документально оформить статический временной анализ (STA) для худших и лучших случаев с целью расчета запасов, учитывая при этом информацию о синхронизации, предоставленную технологическими библиотеками и всеми соответствующими инструментами проектирования и реализации.

8.4.7.2 В случае исключения трактов из STA (вследствие признания их «ложными трактами») или объявления их полицикличными трактами, это решение необходимо обосновать и задокументировать.

8.4.7.3 STA должен удостоверить, что частота каждого синхронизированного блока совместима со всеми трактами, не исключенными из анализа (см. 8.4.7.2), с достаточным запасом в пределах заданной изменчивости микроэлектронной технологии.

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

Примечание — Расфазировка тактовых сигналов — это промежуток времени между поступлениями тактового сигнала в разных местах.

8.4.8 Документация по реализации

По окончании этапа реализации необходимо подготовить соответствующую документацию, в которую включают:

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

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

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

d) временные характеристики (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) предоставить информацию по реализации каждого блока, части блока или модуля (включив эту информацию или ссылку на нее);

b) привести описание сделанного выбора, в частности, в отношении контролепригодности, распределения тактовых сигналов и электропитания, сброса и реализации критических трактов.

8.4.8.2 В документации по реализации необходимо описать и обосновать:

a) ограничения и параметры, передаваемые инструментам;

b) анализ, выполненный для получения гарантии соответствия HPD спецификации требований к нему, и любые выявленные отличия;

c) любые итерации, выполненные при проектировании и реализации;

d) любую избыточность, введенную или удаленную 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 те же результаты (выходные сигналы HPD и результаты верификации), а также проверять полноту и правильность анализа, проведенного после трассировки.

8.4.8.4 В документации необходимо привести сведения об испытаниях, которые следует периодически проводить в ходе эксплуатации с должной аккуратностью в отношении структурных модификаций, введенных инструментами.

8.4.8.5 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 автоматизированная генерация кода

Требования различных компонентов системы можно отразить с помощью инструментов уровня электронной системы (ESL), обеспечивающих текстовое или графическое описание.

В настоящем подразделе даны рекомендации, применимые в случаях, когда описание требований к HPD с помощью инструментов ESL происходит в автоматическом режиме, чтобы частично или полностью сгенерировать конструкцию HPD. Такую генерацию иногда называют высокоуровневым синтезом.

8.5.1 Если спецификацию требований, написанную на языке уровня системы (ESL), применяют для автоматической генерации описания HPD или его части для уровня регистровых передач (RTL), то:

a) сгенерированное описание должно быть понятным и, насколько возможно, простым;

b) это описание должно облегчать понимание поведения устройства, чтобы разработчики аппаратного обеспечения могли быстро идентифицировать ошибки и неоднозначные показания.

8.5.2 Язык системного уровня (ESL) и соответствующие инструменты, в частности, используемые для генерации кода и анализа, должны отвечать требованиям по 8.2.

8.5.3 При несоблюдении требования 8.5.2:

a) описание HPD на языке ESL необходимо перевести в описание на HDL, согласующееся с требованиями 8.2, и это новое описание должно служить основой для последующих мероприятий по проектированию, реализации и верификации;

b) указанные последующие мероприятия должны соответствовать требованиям настоящего стандарта.

8.5.4 Любое несоответствие сгенерированных описаний (таких, как описание RTL, синтезированные, трассированные) требованиям к проектированию и реализации (см. 8.3 и 8.4) должно быть идентифицировано и обосновано.

8.5.5 Если какие-то виды анализов, верификаций или проверок, указанные в разделах 8, 9 и 10, не проводят, то необходимо официально подтвердить, что продукты, не подвергнутые анализу, верификации или проверке, безусловно корректны.

8.5.6 Сгенерированные продукты не допускается изменять путем прямого ручного действия.

8.5.7 Продукты следует генерировать заново, если возникает необходимость изменений, связанная, например, с результатами верификации или проверки.

8.6 Документация

В настоящем подразделе приведены общие требования к документации для проектирования и реализации HPD. Он дополняет требования, установленные для конкретных мероприятий, рассмотренных в 8.1—8.5.

8.6.1 По окончании этапов проектирования и реализации должна быть подготовлена спецификация проекта HPD.

Такой документ служит основой для официальной проверки проекта и реализации и для последующего производства.

8.6.2 Документ должен быть достаточно подробным, чтобы производство могло идти без дальнейших разъяснений.

8.6.3 Документ должен быть построен в соответствии с этапами прохождения процесса. Спецификация проекта может быть представлена как один документ или как комплект документов.

8.6.4 При предоставлении комплекта, состоящего из нескольких документов, каждый документ должен иметь определенную связь с другими документами и касаться строго ограниченного круга вопросов.

8.6.5 Форматы документов следует выбирать в соответствии с конкретными предметами описания, в число которых входят:

a) повествовательное описание;

b) арифметические и логические выражения;

c) графическое представление, схемы и чертежи.

8.7 Пересмотр проекта и реализации

8.7.1 Этап проектирования и реализации должен завершаться официальным пересмотром.

8.7.2 В ходе пересмотра проекта и реализации необходимо проверить документацию, касающуюся проектирования, реализации, анализов и верификаций.

8.7.3 В ходе пересмотра следует проверить полноту и корректность файлов с параметрами и ограничениями, предоставляемых инструментам проектирования и реализации.

8.7.4 В ходе пересмотра необходимо исследовать полноту и корректность статического временного анализа (STA) и анализа после трассировки, чтобы проверить правильность и надежность проекта и реализации с учетом возможных отрицательных последствий, вызванных модификациями, выполненными при помощи инструментов (такими, как упрощение логики или дублирование логического элемента).

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

9 Верификация HPD

9.1 Общие положения

Мероприятия по верификации, касающиеся разработки HPD, которые, как правило, находятся под контролем лица, ответственного за контроль и управление системы безопасности станции, проводят сотрудники, независимые от лиц, осуществляющих проектирование и реализацию HPD. Оптимальным решением является привлечение группы, проводящей верификацию.

С целью получения гарантии соответствия HPD и процесса его разработки плановому заданию могут быть проведены дополнительные мероприятия по верификации третьей стороной. Существует много способов обеспечения ресурсами и проведения независимой верификации, что часто находится в ведении государственного регулирующего органа.

9.1.1 В состав группы верификации должны входить специалисты, не занятые в разработке и обладающие необходимой компетенцией и знаниями. Необходимый уровень независимости однозначно определяется соблюдением нижеследующих требований.

9.1.2 Руководство группы верификации должно быть обособленным и независимым от руководства группы разработки.

9.1.3 Взаимосвязь между группой верификации и группой разработки по вопросам уточняющего характера или с сообщениями о дефектах должна осуществляться официально в письменной форме и с такой степенью детализации, которая позволяет проверить предоставленную информацию.

9.1.4 Целью взаимодействия между указанными сторонами должно быть обеспечение независимости заключения группы верификации.

9.1.5 Обязанности и ответственность группы верификации должны быть четко определены.

9.1.6 Результаты каждого этапа разработки (см. рисунок 2) должны быть верифицированы.

9.1.7 В ходе мероприятий по верификации необходимо подтвердить достаточность спецификации требований к HPD для выполнения требований системы или подсистемы, установленных для данного HPD в спецификации системы или подсистемы.

9.1.8 В ходе мероприятий по верификации необходимо подтвердить правильность выбора и правил использования каждой заготовки интегральной схемы, микроэлектронной технологии, встроенного блока и ПРБ с точки зрения соответствия спецификации требований к компоненту, в состав которого они входят (см. раздел 7).

9.1.9 В ходе мероприятий по верификации необходимо подтвердить достаточность проектной спецификации HPD для установления ее соответствия спецификации требований к HPD.

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

Примечание — Верификация после реализации имеет первостепенное значение для обнаружения возможных неблагоприятных последствий упрощений логики и дублирования логических элементов, которые могут быть выполнены инструментами, а также возможных дефектов, вызванных самими инструментами или их использованием.

9.1.11 Любую производственную деятельность следует начинать на основании верифицированных исходных данных/документов.

9.1.12 Верификацию продукта определенного этапа разработки следует выполнять до начала следующего этапа. В других случаях эту верификацию необходимо проводить перед верификацией продукта следующего этапа.

Допускается проводить подготовительную работу для следующего этапа до того, как будет верифицирован предыдущий этап.

9.1.13 Если исходные данные/документы для какого-то мероприятия были изменены, то это и последующие мероприятия следует повторить в необходимом объеме, чтобы отреагировать на возможное влияние таких изменений.

9.2 План верификации

9.2.1 План верификации должен быть составлен до начала мероприятий по верификации HPD.

9.2.2 В плане должны быть документально зафиксированы все критерии, методы и инструменты, используемые в процессе верификации.

9.2.3 В плане верификации необходимо описать мероприятия, которые должны быть выполнены для оценки каждого элемента HPD, каждого инструмента, используемого в процессе разработки, и каждого этапа, чтобы показать соответствие спецификации требований к HPD.

9.2.4 План верификации должен быть настолько подробным, чтобы группа верификации могла его выполнить и сделать объективное заключение о том, соответствует ли HPD спецификации требований к нему.

9.2.5 План верификации должен быть разработан группой верификации с учетом следующих направлений:

a) выбор и обоснование стратегии верификации в соответствии с особенностями требований, параметрами проектирования и реализации и микроэлектронной технологией;

b) выбор и использование инструментов верификации;

c) проведение верификации;

d) документация по мероприятиям верификации;

e) оценка результатов верификации, полученных непосредственно от инструментов верификации и по итогам испытаний, оценка соблюдения требований по обеспечению безопасности.

9.2.6 В плане верификации необходимо документально зафиксировать каждое испытание, в том числе его цель, ожидаемые результаты и критерии для принятия решения о корректности результата.

9.2.7 Испытания, запланированные с учетом функциональных аспектов, должны предусматривать проверку широкого спектра возможностей HPD.

9.2.8 В плане верификации должны быть указаны все объективные свидетельства, подтверждающие объем тестирования. Для этого необходимо обосновать и документально зафиксировать критерии для оценки тестового охвата, выбранные на основании проектирования и реализации.

9.2.9 Необходимо обеспечить надлежащие условия для рассмотрения и решения всех вопросов, связанных с безопасностью и выявленных в ходе верификации, которая выполнена либо во время разработки изготовителем оборудования контроля и управления, либо во время независимой оценки третьей стороной.

9.2.10 Все вопросы безопасности необходимо решать посредством надлежащих корректирующих модификаций или смягчающих правовых норм.

9.3 Верификация использования предварительно разработанных элементов

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

9.4 Верификация проекта и реализации

9.4.1 В процесс верификации необходимо включить испытания и анализ, направленные на рассмотрение следующих проблем:

a) соответствие проектной спецификации и спецификации требований к HPD в отношении их согласованности и полноты сверху вниз, включая блок и модуль самого нижнего уровня;

b) разбивка проекта согласно иерархии блоков и модулей, а также способ установления иерархии с учетом:

1) контролепригодности для дальнейшей верификации,

2) понятности для групп разработки и верификации,

3) возможности дальнейшей модификации;

c) правильная реализация требований по обеспечению безопасности.

9.4.2 Результат верификации должен быть оформлен документально.

9.4.3 Документация должна содержать выводы и четко обозначать вопросы, требующие разрешения, такие как:

a) элементы, не соответствующие требованиям;

b) элементы, не соответствующие правилам проектирования и реализации;

c) модули, данные, структуры и алгоритмы, не адаптированные должным образом для решения своей задачи.

9.5 Стендовые испытания

9.5.1 Необходимо разработать и документально зафиксировать программу моделирования и тестирования (стендовое испытание). При необходимости стендовое испытание может состоять из нескольких исполнений, когда каждое имеет свою сферу применения и задачу. Так, некоторые испытательные стенды могут быть выделены для испытания модулей, а один или более — для высокоуровневых испытаний.

9.5.2 Испытательный стенд (конструкция) может быть разработан группой проектировщиков для собственных испытательных нужд и использован группой верификации. Однако направления испытания (входные и ожидаемые выходные сигналы), требуемые настоящим стандартом, должны быть разработаны группой верификации, чтобы снизить вероятность маскировки ошибок и получить дополнительное подтверждение понятности и полноты проектной документации.

9.5.3 Необходимо, чтобы испытательный стенд:

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

b) обеспечивал достаточное разрешение по времени при использовании его после реализации для исследования временных аспектов.

9.5.4 Стендовые испытания должны включать испытание всех свойств и особенностей, упомянутых в спецификации требований к HPD и в проектной спецификации, таких как функции, режимы, конечные автоматы, алгоритмы, протоколы.

9.5.5 При проведении стендового испытания следует вводить все необходимые входные данные, последовательности и временные характеристики (синхронизации) и регистрировать все выходные данные, последовательности и синхронизации, получаемые при выполнении испытания, делая это выполнение полностью автоматизированным.

9.5.6 В стендовое испытание следует включать ожидаемые выходные последовательности и синхронизации, а также автоматизированное сравнение с этими параметрами, фактически полученными при выполнении теста (с учетом соответствующих критериев, см. 9.2), чтобы в дополнение к детальным результатам испытания получить на выходе общее заключение «пригоден/непригоден».

9.5.7 Если ввод данных, наблюдения или сравнения требуется выполнять вручную, то:

a) вводимые данные и осуществляемые действия необходимо задокументировать настолько детально, чтобы лица, не занятые в проекте, могли повторить тест. Это может потребовать пошагового определения этапов и значений бит-уровня;

b) необходимо привести документированное обоснование, т. к. ввод данных, наблюдения и сравнения, осуществляемые вручную, чреваты ошибками.

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

9.6 Тестовый охват

9.6.1 Критерии для определения тестового охвата должны быть выбраны и задокументированы.

9.6.2 В документально зафиксированном анализе критериев тестового охвата необходимо показать, что критерии состоятельны в отношении спецификации требований к HPD и параметров проектирования/реализации и что испытательный стенд обеспечивает достаточную возможность наблюдения для принятия решения «пригоден/непригоден» по каждому охваченному испытанием элементу.

9.6.3 Критерии для определения тестового охвата могут быть связаны, например, с инструкциями, решениями, выражениями, путями, конечными автоматами или процессами. Если невозможно достичь тестового охвата, определяемого критерием, например из-за структуры RTL (особенно трудно достичь стопроцентного охвата путей), то должно быть предоставлено документально оформленное обоснование.

Примечание — Путь представляет собой специфическую последовательность ветвлений, имеющих место при выполнении кода.

9.6.4 Каждый модуль, разработанный в рамках проекта, подлежит специфическому для него испытанию.

9.7 Выполнение испытаний

9.7.1 Испытания следует проводить, используя испытательные стенды, после этапа проектирования с описанием на уровне регистровых передач (RTL) для подтверждения его правильности.

9.7.2 Испытания следует проводить после этапа реализации для подтверждения того, что описание после трассировки соответствует ограничениям синхронизации, с учетом информации о временных характеристиках, получаемой с применением инструментов и из библиотек (обратное аннотирование).

9.7.3 Испытания (с помощью моделирования) должны быть проведены 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) должны быть задокументированы.

9.7.5 Анализ любого несоответствия, обнаруженного в ходе испытаний, должен быть задокументирован и предоставлять принятое решение о приемлемости или неприемлемости такого несоответствия.

9.8 Статическая верификация

9.8.1 Необходимо выполнять следующие мероприятия по верификации:

a) проверка типа и синтаксической конструкции;

b) проверка параметров при вызове или инстанцировании модулей, функций, процедур, встроенных блоков и ПРБ;

c) проверка выхода за пределы диапазона;

d) проверка полноты списка сигналов запуска процессов (см. примечание);

e) проверка полноты учета случаев, явно запрограммированных в инструкциях и конструкциях с многочисленными вариантами выбора;

f) обнаружение тупиковых состояний в конечных автоматах;

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

h) логическая и физическая проверка проектных норм, которая тестирует список 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 STA (см. 8.4.7), если основы этих аспектов могут быть математически описаны. В этом случае инструменты, используемые для реализации этих методов, должны:

a) иметь уровень развития и стандартную форму, аналогичные тем, которые установлены требованиями настоящего стандарта для инструментов моделирования;

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

10 Аспекты системной интеграции с участием HPD

10.1 Общие положения

Процесс системной интеграции представляет собой объединение верифицированных компонентов аппаратных средств (и программного обеспечения, если это предусмотрено) в подсистемы и затем в законченную систему. Этот процесс включает два вида действий:

a) системная интеграция: сборка и соединение верифицированных аппаратных компонентов (и компонентов программного обеспечения, если это предусмотрено) для построения промежуточных и конечных целевых объектов. Последовательность сборки, а также степень интеграции последовательных целевых объектов зависит от проектных параметров;

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

В этом разделе приведены требования к системной интеграции, дополняющие требования, указанные в 6.2.5 МЭК 61513, для случаев, когда в интеграции задействованы HPD.

10.2 Аспекты плана системной интеграции с участием HPD

Настоящий подраздел расширяет перечень требований, установленных в 6.3.4 МЭК 61513, подлежащий обязательному исполнению.

10.2.1 Указанный план должен быть подготовлен и документально оформлен на этапах проектирования и реализации и верифицирован на предмет соответствия требованиям к системам класса 1.

10.2.2 Указанный план должен быть подготовлен на достаточно раннем этапе процесса разработки, чтобы все требования к интеграции гарантированно были включены в проект HPD, системы и ее компонентов.

10.2.3 В плане должны быть указаны ссылки на стандарты и процедуры, которым необходимо следовать на этапе системной интеграции.

10.2.4 План должен документально фиксировать те положения плана обеспечения качества системы, которые применимы к системной интеграции.

10.2.5 План интеграции должен устанавливать:

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

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

c) критерии приемки.

10.2.6 В плане системной интеграции необходимо учесть требования, которым должно соответствовать HPD с точки зрения проекта системы, проекта аппаратных средств и проекта программного обеспечения. В план необходимо также включить требования к процедурам и методам управления, касающиеся:

a) управления конфигурацией системы (см. 5.5);

b) системной интеграции;

c) верификации интегрированной системы;

d) устранения дефектов.

10.2.7 План системной интеграции должен отражать как аспекты идентификации, так и аспекты контроля в управлении конфигурацией согласно требованиям, указанным в 6.3.2.3 МЭК 61513.

10.2.8 В процессе верификации взаимодействия HPD с другими компонентами системы могут быть верифицированы некоторые другие составные части на уровне подсистем (вычислительных блоков) или на уровне законченной системы, если это целесообразно. Если верификация путем тестирования на этих уровнях невозможна, то:

a) все требования к HPD необходимо верифицировать другими средствами (например, тестирование методом прозрачного ящика);

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

10.2.9 Все взаимозависимости между верификацией HPD и верификацией интегрированной системы должны быть документально зафиксированы в плане системной интеграции.

10.3 Особые аспекты системной интеграции

Особые процедуры системной интеграции устанавливают в зависимости от характеристик архитектуры системы.

10.3.1 В плане системной интеграции приводят ссылки на процедуры, которые должны быть установлены для выполнения следующих мероприятий:

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

b) интеграция HPD в систему (т. е. размещение компонента, конфигурирование, монтажные соединения);

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

d) документирование результатов процесса интеграции и конфигурации системы по итогам тестирования;

e) представление окончательной версии интегрированной системы для тестирования пригодности.

10.3.2 Если для устранения дефекта необходима модификация верифицированного HPD или проектной спецификации, то это должно быть проведено согласно процедурам, указанным в 10.5.

10.3.3 Любые дефекты, выявленные во время системной интеграции, которые являются лишь следствием ошибок в самом интеграционном процессе и которые не затрагивают документированную информацию о HPD, необходимо исправлять путем обновления плана системной интеграции.

10.4 Верификация интегрированной системы

Верификация интегрированной системы определяет, насколько корректно интегрированы в систему верифицированные компоненты и подсистемы, совместимы ли они и функционируют ли они надлежащим образом.

10.4.1 Необходимо, чтобы система была законченной, насколько это целесообразно для данной верификации.

10.4.2 Сценарии, отобранные для верификации системы, должны обеспечивать:

a) проверку всех интерфейсов HPD и всех основных операций;

b) проверку всех параметров интерфейса HPD, приведенных в спецификации требований и в проектной спецификации, таких как протоколы, последовательности, синхронизации и электрические характеристики;

c) достаточный охват, позволяющий подтвердить, что HPD функционирует так, как требуется во всех достижимых для системы ситуациях.

10.4.3 В плане системной интеграции должны быть указаны тесты, которые следует провести для проверки соответствия каждому требованию к интерфейсу HPD.

10.4.4 Критический анализ программы испытаний интегрированной системы и оценку результатов испытаний должна осуществлять группа верификации, знающая спецификацию системы.

10.4.5 Оборудование, используемое для верификации системы, должно быть откалибровано надлежащим образом.

10.4.6 Используемые программные инструменты верификации должны соответствовать требованиям раздела 15, касающимся инструментов верификации.

10.4.7 Верификация интегрированной системы должна подтвердить, что все компоненты системы (такие, как блоки обработки и устройства связи) обладают соответствующими эксплуатационными характеристиками.

10.5 Процедуры устранения дефектов

10.5.1 Процедуры должны соответствовать требованиям, установленным в 6.3.2.4 («Процедуры устранения дефектов») МЭК 61513.

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

10.6 Аспекты отчета о тестировании интегрированной системы, связанные с HPD

10.6.1 Отчеты о тестировании должны соответствовать требованиям, установленным в 6.4.5.2 МЭК 61513.

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

11 Аспекты валидации системы, связанные с HPD

11.1 Общие положения

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

a) Испытания с целью валидации системы и HPD должны быть проведены в соответствии с требованиями к системам класса 1.

b) Валидационные испытания следует проводить на системе в конфигурации ее финальной сборки, включая окончательную версию устройства HPD.

11.2 Аспекты плана валидации системы, связанные с HPD

11.2.1 Валидацию системы следует проводить в соответствии с официальным планом валидации системы.

11.2.2 В плане следует определить статические и динамические тестовые сценарии.

11.2.3 Разработку плана валидации системы и оценку результатов валидации должны проводить специалисты, не участвовавшие в проектировании и реализации.

11.3 Валидация системы

11.3.1 Система должна быть подвергнута тестированию с помощью статических и динамических входных сигналов, имитирующих нормальную эксплуатацию, эксплуатацию в различных прогнозируемых обстоятельствах и эксплуатацию в аварийных условиях, требующих действий.

11.3.2 Тестирование каждой функции категории А системы необходимо осуществлять путем серии испытаний, подтверждающих каждый необходимый выходной сигнал одиночным или комбинированным способом.

11.3.3 Испытания должны:

a) охватывать все функции, предусмотренные спецификацией требований к HPD, во всех режимах (см. 6.2);

b) охватывать все диапазоны сигналов и расчетных параметров, если для этого есть весомые основания;

c) обеспечивать всестороннюю проверку процесса выбора, других одиночных или комбинированных логических узлов;

d) обеспечивать проверку всех сигналов аварийного отключения или защитных сигналов в конфигурации окончательной сборки;

e) обеспечивать проверку необходимой реакции на определенные отказы;

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

11.3.4 Кроме того, в плане валидации системы должны быть указаны значения входных сигналов, ожидаемые выходные сигналы и критерии приемки.

11.3.5 Оборудование, используемое для валидации, должно быть соответствующим образом откалибровано и сконфигурировано (параметры аппаратных средств и программного обеспечения).

11.4 Аспекты отчета о валидации системы, связанные с HPD

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

11.4.2 В отчете необходимо указать аппаратные средства, программное обеспечение (в соответствующих случаях), используемую конфигурацию системы, используемые конфигурации инструментов и используемое испытательное оборудование (включая его калибровку и имитируемые модели) в соответствии с 6.4.6.2.b МЭК 61513.

11.4.3 В отчете необходимо также указать любые несоответствия, выявленные при испытании.

11.4.4 В отчете должны быть обобщены результаты валидации системы.

11.4.5 В отчете должна быть представлена оценка соответствия системы всем требованиям.

11.4.6 Результаты необходимо сохранять в такой форме, чтобы их могли верифицировать специалисты, не занятые непосредственно в процессе валидации.

11.4.7 Моделирование станции и ее систем, используемое для валидации, необходимо документально зафиксировать.

11.5 Процедуры устранения дефектов

К аспектам валидации системы, связанным с HPD, также применяют требования, указанные в 10.5.

12 Модификации

12.1 Модификация требований, проекта или реализации

12.1.1 Процесс внесения изменений и его документальное оформление должны соответствовать требованиям МЭК 61513 (6.2.8 и 6.4.7), МЭК 60987:2007 (раздел 12) и МЭК 60880:2006 (раздел 11).

12.1.2 Все относящиеся к процессу документы должны быть верифицированы согласно требованиям раздела 9 специалистами, не занятыми в проектировании или реализации модификации.

12.2 Модификация микроэлектронной технологии

Поставщик может обновлять микроэлектронную технологию (например, использовать новую версию чистой ПЛИС, чтобы увеличить быстродействие или уменьшить размер кристалла). Даже если новая часть заявлена как совместимая, это не означает, что любая схема будет функционировать одинаково с прежним и обновленным устройствами.

12.2.1 Процесс приемки (раздел 7) следует провести снова, включая в него при необходимости все соответствующие этапы жизненного цикла в зависимости от выявленных различий.

12.2.2 Должны быть снова проведены необходимые мероприятия по верификации, оформленные документально должным образом, чтобы гарантировать соответствие требованиям всех функциональных, электрических и временных характеристик.

12.2.3 Даже если новые и прежние части имеют одинаковую логическую конфигурацию и совместимы по выводам, следует оценить и документально зафиксировать необходимость повторной генерации файлов программирования (например, из-за различий синхронизации или напряжений программирующих импульсов).

13 Производство HPD

13.1 Общие положения

В область применения настоящего стандарта не входит проектирование и изготовление предварительно разработанных микроэлектронных ресурсов (например, чистых ПЛИС), используемых в качестве исходного материала в процессе разработки HPD. В настоящем стандарте термин «производство» обозначает заключительный этап, на котором поставляют интегральную схему, готовую к применению в СКУ.

13.2 Производственные испытания

13.2.1 В ходе испытаний необходимо проверить на соответствие требованиям функции HPD, а также его временные 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 Необходимо получить подтверждение, что испытания, выполненные поставщиком интегральной схемы, удовлетворяют требованиям (см. 13.2.1). Производителю СКУ не нужно повторять ис-

пытания, выполненные поставщиком интегральной схемы, или знать соответствующие направления тестов.

13.2.3 Если требование 13.2.2 не выполнено, производитель СКУ должен провести дополнительные испытания (с документально зафиксированными входными сигналами, ожидаемыми выходными сигналами и критериями приемки), чтобы подтвердить соответствие требованиям (см. 13.2.1).

13.2.4 При производственных испытаниях, выполняемых на уровне плат (например, проверке пайки после сборки HPD на печатной монтажной плате), необходимо проверить работоспособность интерфейса данной части (например, провести испытания контактов на ошибку типа «постоянный 0», общие функциональные испытания).

13.2.5 Каждая изготовленная часть должна пройти производственные испытания или должна быть признана непригодной.

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

13.3 Программирующие файлы и программирование

13.3.1 Программирующие файлы должны содержать коды обнаружения ошибок, а программирующее оборудование должно их проверять.

13.3.2 Для каждой изготовленной части необходимо:

a) проверить конфигурацию после программирования;

b) сохранить соответствующую информацию для возможности трассировки (такую как номер партии, файл системного журнала программирования, параметры программируемых переключателей до и после программирования.

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

13.3.4 Следует использовать только те инструменты, на которые поставщик интегральной схемы дает гарантию и обеспечивает поддержку.

14 Аспекты установки, ввода в эксплуатацию и эксплуатации, связанные с HPD

a) Процессы установки, ввода в эксплуатацию и эксплуатации, а также их документальное оформление должны соответствовать требованиям МЭК 61513 (6.2.7 и 6.3.6), МЭК 60987:2007 (разделы 10 и 13) и МЭК 60880:2006 (раздел 12).

b) Согласно МЭК 60671 оборудование и СКУ, выполняющие функции категории А, должны проходить регулярные испытания для подтверждения надлежащего функционирования. Для достижения необходимого для HPD охвата испытаниями следует использовать соответствующие методики испытаний в целях повышения контролепригодности, например периферийное сканирование.

15 Программные средства для разработки HPD

15.1 Общие положения

К программным средствам, используемым при разработке HPD, применяют требования, установленные в разделе 14 МЭК 60880:2006, за исключением требований, указанных в 14.3.4.3, 14.3.4.4 и 14.3.4.5.

Примечания

1 Техническая оценка компании — поставщика инструментов (не ограниченная только обеспечением качества) является приемлемым способом принятия решения о выполнении требования, указанного в 14.2.2 МЭК 60880:2006, при условии наличия соответствующей документации.

2 Такая характеристика программных средств, как «надежность», которой посвящен раздел 14 МЭК 60880:2006, в настоящем стандарте означает «достоверность» или «корректность».

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

4 Библиотеки, интегрированные в инструментальные средства, могут быть оценены в контексте оценки инструментов.

5 Верификация выходных данных инструментальных средств, указанная в 14.3.2.4 МЭК 60880:2006, может быть выполнена различными способами, например с помощью имитационной модели, отличной от набора синтезирующих инструментов.

15.2 Дополнительные требования к инструментам проектирования, реализации и моделирования

15.2.1 Программные средства должны обеспечивать доступ к параметрам, управляющим логическим синтезом и реализацией (например, через настройки).

15.2.2 Программные средства не должны без предупреждения добавлять структуры, не прослеживаемые непосредственно до операторов исходных программ HDL (например, дублировать логический элемент для соответствия требованию синхронизации).

15.2.3 Проектировщики должны предварительно ознакомиться с программными средствами, в частности: они должны знать, как эти средства функционируют на структурах и схемах, используемых в проекте.

15.2.4 Если программное средство требует аргументы командной строки, то они должны быть в файле сценария (помещенном под управлением конфигурацией) во избежание ошибок ручного вызова.

Примечание — Вышеизложенное полезно не только для согласованности данных, но и для оценки происхождения дефекта, который может быть в исходном коде, в программном средстве или параметрах программного средства. Это также может быть необходимо при оценке возможности ООП, обусловленного применением инструментов проектирования и реализации.

15.2.5 При переходе на новую версию программного средства, которое отвечает за преобразование проектной информации (например, за логический синтез или размещение и трассировку), все соответствующие мероприятия по моделированию, анализу и верификации необходимо выполнить снова.

Примечания

1 В ходе задокументированного анализа можно обосновать, что данная модификация программного средства не может влиять на вышеупомянутые мероприятия, например на коррекцию некоторого несогласованного поведения в графическом пользовательском интерфейсе программного средства.

2 Мероприятия, которые были завершены до изменения программного средства, повторять не надо.

16 Сегментация или разделение конструкции

16.1 Предварительная информация

На некоторых HPD возможны проектирование и реализация схем, размещенных физически в разных зонах интегральной схемы, взаимно друг с другом не связанных или имеющих минимальные связи и не использующих общие аппаратные ресурсы. Некоторые HPD поддерживают такие зоны, иногда называемые озерами, с неиспользуемым или непригодным для использования пространством между ними. К числу преимуществ сегментации или разделения конструкции можно отнести реализацию вспомогательных или поддерживающих функций (что не должно служить заменой для резервированных каналов проекта на системном уровне).

16.2 Вспомогательные функции или функции поддержки

16.2.1 Общие сведения

Обычно вспомогательные функции или функции поддержки, реализуемые HPD, даже если они не относятся к функциям категории А, потенциально могут препятствовать выполнению функций категории А данного HPD. Таким образом, если невозможно подтвердить соответствие требованиям 16.2.2, вспомогательные функции или функции поддержки следует разрабатывать, реализовывать и верифицировать в соответствии с требованиями настоящего стандарта (т. е. как функции категории А).

16.2.2 Разделение вспомогательных функций или функций поддержки, относящихся к категории, отличной от категории А

Настоящий стандарт устанавливает, что при применении особых критериев проектирования и разделении HPD можно обеспечить независимость вспомогательных функций или функций поддержки от функций категории А и невозможность их ненадлежащего вмешательства в выполнение функций

категории А. В таких случаях вспомогательные функции или функции поддержки могут быть реализованы HPD класса 1 без той степени строгости, которая требуется для функций категории А, при условии соблюдения следующих требований:

a) необходимо подтвердить, используя проект, реализацию, оценку и регулярную верификацию, что выполнение или отказ вспомогательных функций или функций поддержки не могут прямо или косвенно влиять 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 подсоединенной линии и т. д.);

b) такое подтверждение должно учитывать все возможные причины помех, например функциональные, электрические, электромагнитные, тепловые и т. д.;

c) при этом зоны интегральной схемы, используемые для реализации таких вспомогательных функций или функций поддержки, должны быть физически отделены от зон, используемых для реализации функций категории А;

d) в случае модификации HPD следует подтвердить, что требования 16.2.2 продолжают соблюдаться;

e) интерфейс между схемами, реализующими функции категории А и вспомогательные функции или функции поддержки, должен быть простым и полностью верифицируемым;

f) данные, получаемые функциями категории А от вспомогательных функций или функций поддержки, должны быть ограничены значениями статических параметров (например, калибровочные постоянные, заданные значения);

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

h) необходимо принимать соответствующие меры безопасности (например, безопасные протоколы обмена данными) для любого информационного взаимодействия между функциями категории А и вспомогательными функциями или функциями поддержки, чтобы все ошибки передачи данных были обнаружены, надлежащие меры реагирования для обеспечения безопасности были предприняты или получение корректных данных было подтверждено.

17 Защита HPD от отказа по общей причине

17.1 Предварительная информация

В любой процесс проектирования и реализации могут быть внесены систематические дефекты из-за ошибки человека. Такие дефекты могут быть внесены также при проектировании и реализации HPD (как в разрабатываемой части, так и в разработанной ранее и включенной в состав проекта). Следовательно, существует вероятность воздействия на HPD скрытых систематических дефектов, которые при возникновении некоторых инициирующих событий могут привести к ООП многих элементов проекта HPD.

Возможность возникновения ООП в многоэлементных системах рассматривается в стандартах более высокого уровня подкомитета МЭК ПК 45А, в частности, в МЭК 61513 и МЭК 62340. В настоящем стандарте рассматривается возможность возникновения ООП, связанная с использованием проекта многоэлементного HPD в подобной системе. Как указано в разделе 1, настоящий стандарт устанавливает процессы разработки и верификации HPD, а также требования к ним, позволяющие минимизировать вероятность систематических дефектов HPD и, как следствие (поскольку такие дефекты HPD могут стать причиной ООП), минимизировать возможность ООП, обусловленных использованием HPD.

Ниже приведены дополнительные требования, направленные на защиту от систематических дефектов, которые могут привести к ООП, обусловленным применением HPD.

17.2 Требования

17.2.1 Аспекты процессов разработки HPD, связанные с возможностью ООП многих элементов проекта HPD (которые еще не были рассмотрены в настоящем стандарте), должны отвечать в применимых случаях соответствующим требованиям МЭК 60880:2006, 13.1 (при этом термин «программное обеспечение» следует заменить на «HPD»).

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

17.2.2 Согласно требованиям МЭК 60880:2006, указанным в 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.7 и 13.3.8, в применимых случаях необходимо выполнить анализ, направленный на изучение аспектов процессов разработки HPD, связанных с возможностью ООП многих элементов проекта HPD (которые еще не были рассмотрены в настоящем стандарте).

Примечание — Некоторые требования указанных пунктов относятся к ООП на уровне архитектуры СКУ, хотя было бы правильнее включить их в документ более высокого уровня, рассматривающий вопросы ООП, а именно — в МЭК 62340. В целях сохранения структуры серий стандартов подкомитета МЭК ПК 45А рекомендуется при следующем пересмотре перенести эти требования в МЭК 62340.

Приложение А
(справочное)

Документация

В данном приложении приведен типичный перечень документов для каждого из основных разделов настоящего стандарта. Материалы могут быть представлены в виде комплекта документов, отличающихся от предложенных в этом приложении, при условии четкого обозначения разделов.

А.1 Проект

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

А.2 Спецификация требований к HPD

a) спецификация требований;
b) отчет по анализу требований;
c) отчет по результатам проверки.

А.3 Приемка заготовок интегральных схем, встроенных блоков и ПРБ

a) спецификация требований к компонентам;
b) пользовательская документация по безопасности;
c) прочая документация по компоненту, в том числе такая информация, как спецификация, проект, тестирование, практика применения;
d) отчет об анализе;
e) документ, содержащий правила использования;
f) отчет по результатам приемки.

А.4 Проектирование и реализация HPD

a) спецификация проекта, в том числе:
1) описание разбивки на основные модули, проектных решений по защите, идентификации микроэлектронной технологии, инструментов, встроенных блоков и ПРБ,
2) детальное описание проекта, включающее:
- описание на уровне регистровых передач,
- организационные опции (модули, подмодули, интерфейсы, протоколы и т. д.),
- предварительные электрические и временные характеристики,
3) описание реализации, в том числе:
- описание на уровне логических элементов (список связей), специальное технологическое описание для производства, обратное аннотирование,
- реализация модулей, критических сигналов и распределения электропитания, возможные инструменты, вспомогательные файлы, используемые для реализации, такие как файлы ограничений,
- отчет по анализу после трассировки, отчет по STA,
- анализ контролепригодности, направления тестов при периодических испытаниях,
- электрические характеристики и подробные синхронизации;
b) отчеты по результатам проверки.

А.5 Верификация HPD

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

А.6 Аспекты системной интеграции, связанные с HPD

a) план интеграции, включающий стратегию и процедуры интеграции, интерфейс управления конфигурацией, тестовые сценарии;
b) особые аспекты отчета об испытании интегрированной системы, включая определение компонентов и инструментов, результаты и анализ испытаний, выявленные дефекты и их устранение;
c) отчет о проверке интеграции.

А.7 Аспекты валидации системы, связанные с HPD

a) план валидации, в том числе тестовые сценарии;

b) отчет, включающий определение компонентов и инструментов, результаты испытаний, анализ испытаний, выявленные дефекты и их устранение.

А.8 Внесение изменений

Типичный перечень документов, касающихся процесса внесения изменений, приведен в приложении F МЭК 60880:

a) отчет об отклонениях;

b) запрос на внесение изменений;

c) отчет о внесении изменений;

d) журнал контроля за внесением изменений.

Кроме того, необходимо обновлять документы, относящиеся к этапам разработки, на которые повлияло внесение изменений.

А.9 Производство HPD

a) документ, содержащий описание производственных испытаний;

b) документ, содержащий результаты производственных испытаний, идентификационные данные составных частей и сведения по программированию составных частей.

А.10 Программные средства для разработки HPD

a) отчет о выборе средств (анализ поддержки средств, оценка, приемка, ограничения применения);

b) документ, описывающий стратегию внесения изменений, обновления или замены.

Приложение В
(справочное)

Разработка HPD

Разработку HPD, рассматриваемую в настоящем стандарте, выполняют с помощью языков описания аппаратных средств и инструментов проектирования, функционирующих на рабочих станциях, в соответствии с алгоритмом, представленным в этом приложении в общем виде для облегчения понимания соответствующих разделов настоящего стандарта.

В.1 Установление дополнительных требований на уровне электронных систем

Принятие требований иногда осуществляют на основании высокоуровневого описания системы, в состав которой входит разрабатываемое HPD. Это описание включает в себя другие компоненты аппаратного и программного обеспечения. Каждый компонент представлен поведенческой моделью, и эти модели осуществляют обмен информацией по каналам связи, имитируя проектируемую систему.

Этот уровень описания, называемый уровнем электронной системы (ESL), использует такие языки описания системы, как SystemC или System Verilog.

Такое описание, как правило, выполняют (моделируют) с помощью функциональных тестовых сценариев для оценки применимости различных вариантов системной архитектуры и выбора наилучшего варианта, а также для установления в конечном итоге требований к каждому компоненту, включающему HPD, с учетом поведенческой модели и интерфейса.

В.2 Проектирование

Исходя из требований данный этап первоначально нацелен на определение основных принципов проектирования, таких как разделение на предварительно разработанные или заказные модули, организация самоконтроля и идентификация микроэлектронной технологии (включая встроенные блоки) и ПРБ, которые могут быть использованы.

Затем создают описание на уровне регистровых передач (RTL) и проводят испытание с помощью средств моделирования. Используют такие языки описания аппаратных средств, как VHDL или Verilog. В большинстве случаев это не зависит от микроэлектронной технологии, которая будет применяться.

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

Описание RTL имеет структурные аспекты, показывая логические связи между модулями, которые могут быть специально спроектированы или взяты из библиотек. Это описание также содержит поведенческие аспекты, что позволяет описать функцию модуля, используя средства алгоритмических описаний. Описание RTL выполняют, используя язык описания аппаратных средств (HDL), как правило, VHDL (IEEE 1076) или Verilog (IEEE 1364).

Описание RTL должно быть синтезируемым, что означает возможность его автоматического преобразования в набор взаимосвязанных электронных схем. Для достижения этого свойства проектировщик использует лишь подмножество языка HDL, а полнофункциональный язык может быть использован, например, для создания среды моделирования.

Параллельно с проектированием имеет смысл разработать испытательный стенд на том же языке: RTL-описание HPD включают в более широкую программу HDL, которая отправляет его входные последовательные сигналы и считывает его выходные сигналы с целью его тестирования посредством моделирования. При разработке испытательного стенда могут быть использованы несинтезируемые языковые функции для упрощения разработки тестов (например, доступ к файлам, печать, явное управление временем). Затем испытательный стенд используют для проверки описания RTL; он также может быть соотнесен с различными инструментами для генерации тестов и измерения охвата.

Для обеспечения дополнительного средства верификации предложены инструменты статического анализа. Как правило, они позволяют подтвердить, включены или не включены некоторые ожидаемые свойства в описание HDL. Примерами статического анализа являются проверка свойств, верификация на основе утверждений, проверка эквивалентности различных уровней проектирования (например, RTL и списка связей), или STA.

В.3 Реализация

Начиная с описания RTL создают электронное описание, обеспечивающее фактическую реализацию с использованием выбранной электронной технологии. Основными этапами реализации являются логический синтез, размещение и трассировка.

Различные семейства компонентов (такие, как ПЛИС), стандартные ячейки памяти и т. д., обеспечивают различные предварительные характеристики физического поведения конечного продукта. Из этого следует, что хотя указанные ниже действия объективно необходимы, они могут быть автоматически поддержаны соответствующими

инструментами или нет. Далее приведено краткое описание указанных действий для проектирования на основе стандартных ячеек данных.

Посредством логического синтеза описание RTL преобразуют в сеть логических ячеек микроэлектронной технологии, называемую списком связей. В зависимости от этой микроэлектронной технологии эти логические ячейки могут представлять собой только элементарные логические операторы (такие как И, ИЛИ) или включать более широкие функции (например, счетчики).

Несмотря на то что для синтеза используют инструменты, аналогичные программным компиляторам, проектировщик управляет процессом, предоставляя информацию об ожидаемых характеристиках (таких, как частота синхронизации, задержка между двумя сигналами, энергопотребление) и о том, как обрабатывать критические сигналы, например тактовые сигналы. Указанную информацию, как правило, хранят в файлах ограничений, которые могут быть очень большими. Следовательно, их обработка может быть затруднительной, и ошибка или пропуск могут привести к созданию схемы, страдающей неявными трудновоспроизводимыми дефектами, 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 устанавливают связи между ними с учетом технологических ограничений (существования и емкости предопределенных трассировочных каналов), а также ограничений применения (например, максимальной задержки распространения между двумя заданными узлами).

По мере увеличения числа логических элементов число связей между ними возрастает. Таким образом, становится необходимым размещать на кристалле все большее число связей. Кроме того, требования к скорости распространения, как правило, вынуждают делать некоторые тракты короче. Последнее ограничение может привести к изменениям в размещении некоторых логических элементов, что в свою очередь отражается на всей схеме трассировки. Поиск наилучшего решения является очень трудной задачей (с точки зрения вычислительных возможностей), поэтому возможен только поиск приближенных решений с помощью инструментов, которые нуждаются в использовании наиболее современных и эволюционных алгоритмов.

После размещения и трассировки создают описание в формате, который зависит от используемой микроэлектронной технологии. Поскольку на данном этапе схема физического расположения уже известна, можно более точно оценить время распространения сигналов с учетом сопротивления и емкости каждого тракта. Эту информацию обычно используют для обратного аннотирования описания, чтобы смоделировать его на испытательном стенде с реальным временем распространения для логических элементов и проводных соединений.

Кроме того, поставщик микроэлектронной технологии предлагает время распространения сигнала для логических элементов, включенных в ее библиотеку, используя форматы типа VHDL-VITAL (стандарт IEEE 1076.4). Эту информацию о синхронизации включают в описание списка связей как «обратное аннотирование» и учитывают при моделировании после реализации.

В дополнение к верификации посредством моделирования после реализации проверять время распространения сигнала, а также эквивалентность различных уровней описания позволяют инструменты статического временного анализа (STA).

В.4 Типы специализированных интегральных схем

В.4.1 Общие положения

С развитием технологий появляется много вариантов специализированных интегральных схем, поэтому настоящий стандарт устанавливает требования, основанные на принципах, а не на конкретных особенностях каждого варианта.

В данной части приложения дан обзор основных доступных вариантов (в качестве примечания: в промышленности их названия не всегда используют единообразно).

Теоретически любую вычисляемую функцию можно реализовать одним типом тщательно выбранного логического элемента, такого как «И-НЕ» [«А и-не В» означает «не (А и В)»]. Следовательно, диапазон функций, которые можно реализовать в данной схеме, зависит главным образом от ее размера (количества логических элементов) и от ее внутренней связанности, которая позволяет более или менее эффективно использовать элементы.

В.4.2 Программируемая логическая матрица (ПЛМ)

ПЛМ представляют собой малоразмерные устройства, как правило, организованные в виде массива ИЛИ/И, которые используют для реализации логических уравнений, имеющих форму суммы произведений, например результат = (А и В и не С) или (не В и не С) или (D).

ПЛМ изготавливают как специализированные изделия с конфигурируемыми соединениями, как правило, путем прожига плавких вставок или, в некоторых случаях, путем конфигурирования перепрограммируемых переключателей.

Структура И является программируемой, т. е. выражение произведения перед программированием имеет следующий вид: (А и не А и В и не В и С и не С, и т. д.), где каждый член выражения соответствует одному конфигурируемому соединению. Согласно функциональным требованиям ненужные члены удаляются и получается, например, (А и не С).

Структура ИЛИ является фиксированной: входные данные структуры ИЛИ — это фиксированное число таких программируемых произведений, например (A и не C) или (A и не B) или (D).

Для конфигурирования ПЛМ обычно используют низкоуровневые языки, например PALASM: проектировщик вводит логические уравнения, которые необходимо реализовать, а инструмент переводит их в карту соединений. На таких языках невозможно создать такое же поведенческое описание, как на языках VHDL или Verilog.

ПЛМ, как правило, предоставляют несколько входов и выходов (например, 10 входов, 8 выходов), и они эквивалентны не более чем нескольким сотням логических элементов. По причине своего ограниченного размера они не входят в область применения настоящего стандарта.

В.4.3 ПЛУ, СПЛУ (программируемое логическое устройство, сложное ПЛУ)

ПЛУ и СПЛУ представляют собой большие массивы взаимосвязанных ПЛМ, но новые семейства могут предлагать дополнительные свойства.

Как и у ПЛМ, в их основе лежит сумма произведений с фиксированной структурой, поэтому трассировка сигнала от входа до выхода фиксирована, а время задержки распространения достаточно постоянно. Разумеется, это свойство может быть утрачено при реализации предлагаемых дополнительных функциональных возможностей, таких как линии обратной связи или специализированная логика.

СПЛУ достигают размеров, эквивалентных размерам десятков тысяч логических элементов.

В.4.4 ПЛИС

ПЛИС организованы как большое число программируемых логических блоков, предоставляющих в том числе возможности для комбинаторной логики и хранения. Данные блоки взаимосвязаны посредством иерархии программируемых внутренних соединений, а также имеют контактные площадки ввода-вывода (направление, импеданс, напряжение и сохранение в памяти обычно подлежат программированию). Конкретные линии связи предназначены для критических сигналов, таких как сигналы синхронизации. Кроме того, ПЛИС могут содержать специализированные логические блоки, такие как память, ядро процессора, стандартные интерфейсы и т. д.

Для ПЛИС эквивалентность логических элементов на практике неактуальна, поскольку в связи со сложностью и разнообразием их структур трудно прогнозировать, сколько блоков необходимо для выполнения конкретной функции. Некоторые ПЛИС включают в себя сотни тысяч программируемых блоков, сотни входов/выходов и выполнены из миллиардов транзисторов.

ПЛИС могут сохранять свои функции («конфигурацию») с помощью таких средств, как:

a) статическая оперативная память (конфигурация изменяемая, информация копируется при запуске из внешней памяти);

b) флэш-память (конфигурация сохраняется в неизменяемых элементах, но с перепрограммируемой внутренней памятью);

c) антипрожигаемая плавкая вставка (конфигурация постоянна; такие устройства являются однократно программируемыми).

Чувствительность конфигурации к единичному отказу и нейтронному/альфа-излучению высока для статической оперативной памяти, низка для флэш-памяти и очень низка для антипрожигаемых плавких вставок.

В.4.5 Матрица логических элементов или предварительно созданная интегральная схема с диффузионными областями

Поставщик интегральных схем заранее подготавливает стандартные интегральные схемы, в которых все транзисторы уже установлены, но не соединены. Конкретную функцию, которую необходимо реализовать, генерируют путем создания специфических межтранзисторных связей.

Такой подход подразумевает единовременные затраты, связанные с производством специфических масок для металлических слоев (выполнением межсоединений), но может предполагать более низкую стоимость изготовления по сравнению с ПЛИС, поскольку для реализации программируемой схемы не используют кремний. Однако похоже, что ПЛИС все более вытесняют эту технологию.

В.4.6 Стандартные элементы

Поставщик предлагает микроэлектронную технологию и проекты стандартных логических элементов, создаваемых с ее помощью, таких как элементарные комбинаторные элементы, триггеры, сумматоры, счетчики и т. д. Эти элементы имеют известные характеристики, такие как площадь, входной ток, емкость и задержка распространения сигнала. Элементы 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 элементов описаны в технологической библиотеке, которую предоставляют проектировщику СКУ. Этой библиотекой пользуются при логическом синтезе (см. раздел В.3), когда описание RTL преобразуют в список связей этих элементов, которые затем размещают на интегральной схеме и соединяют. После завершения функциональных и технологических верификаций изготавливают маски, необходимые для производства интегральных схем, и можно начинать производство.

Такой подход подразумевает более высокие единовременные затраты по сравнению с использованием матриц логических элементов, поскольку все маски специфические, но одновременно предполагает более низкую стоимость изготовления, так как размер интегральной схемы будет как раз таким, какой необходим. Наличие различных логических элементов каждого типа, позволяющее находить оптимальные решения по таким проблемам, как быстродействие, площадь или энергопотребление, обеспечивает более высокий уровень оптимизации каждой

части проекта, но все же под контролем проектировщика средств контроля и управления и при условии применения только инструментов HDL.

В.4.7 Полностью заказная СИС или необработанная СИС

Данная технология подразумевает специальное проектирование всех аспектов интегральной схемы, вплоть до уровня транзисторов, с использованием специализированных инструментов. Это означает очень высокие единовременные затраты, что требует экономического обоснования. Специализированные интегральные 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	IDT	ГОСТ Р МЭК 60671—2021 «Системы контроля и управления, важные для безопасности атомных станций. Контрольные испытания»
IEC 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC 60987:2007	—	*
IEC 61513:2011	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 62138	—	*
IEC 62340	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

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

- IDT — идентичные стандарты.

Библиография

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

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

IEC 62342, Nuclear power plants. Instrumentation and control systems important to safety. Management of ageing

ISO 9001, Quality management systems. Requirements

ISO/IEC 25000[3)], Software engineering. Software product Quality Requirements and Evaluation (SQuaRE). Guide to SQuaRE

[1)] Заменен на IEC/IEEE 60780-323:2016 «Nuclear facilities — Electrical equipment important to safety — Qualification» («Атомные электростанции. Электрооборудование, важное для безопасности. Квалификация»).

[2)] Действует IEC 61226:2020 «Nuclear power plants — Instrumentation, control and electrical power systems important to safety — Categorization of functions and classification of systems» (Атомные электростанции. Системы контроля и управления и электроэнергетические системы, важные для безопасности. Категоризация функций и классификация систем).

[3)] Действует ISO/IEC 25000:2014 «Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE» [Системная и программная инженерия. Требования и оценка качества систем и программных средств (SQuaRE). Руководство по SQuaRE].

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции, системы контроля и управления, программируемые устройства, язык описания аппаратных средств, уровень электронных систем, программируемая логическая интегральная схема, программируемое логическое устройство

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.Ю. Литовкиной*

Сдано в набор 23.12.2021. Подписано в печать 19.01.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

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

gost.e-ecolog.ru