БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра ЭТТ

РЕФЕРАТ

На тему:

"Встроенный контроль и диагностика цифровых

устройств. Методы повышения контролепригодности

цифровых устройств"

МИНСК, 2008

Качество контроля и диагностики зависит не только от технических характеристик контрольно-диагностирующей аппаратуры, но и в первую очередь от тестопригодности (контролируемости) самого испытываемого изделия. Это означает, что качество проверки во многом предопределяется качеством разработки изделий. Простейшее решение повышения качества контроля – это вывод некоторых внутренних точек изделия на внешний разъем. Однако число свободных контактов на разъеме ограничено, поэтому указанный подход редко оказывается доступным или достаточно эффективным. Более приемлемое решение связано с размещением на плате дополнительных функциональных элементов, предназначенных для непосредственного получения или накопления информации о состоянии внутренних точек и последующей ее передачи на обработку по требованию анализирующего устройства (внешнего или также встроенного).

Сигналы, возникающие в процессе функционирования основной и контрольной аппаратуры, размещенной вместе на одном печатном модуле или кристалле ИС, сопоставляются по определенным правилам. В результате такого сопоставления вырабатывается информация о правильном функционировании контролируемого узла. В качестве избыточной аппаратуры может быть использована полная копия проверяемого узла (рис.1, а). При этом производиться простейшее сравнение двух одинаковых наборов кодов. С целью уменьшения объема дополнительной контрольной аппаратуры используют более простые контрольные устройства с избыточным кодированием (рис.1, б), но зато при этом усложняются способы получения контрольных соотношений.

Рис. 1. Схемы встроенного контроля с избыточным дублированием аппаратурной части (а) и с избыточным кодированием операций:

ОУ

# КУ

# УС

Х

Y

Z

а)

**О**У

УД

УК

УОКК

УС

Х

Y

Z

б)

ОУ – основное устройство; КУ – контрольное устройство;

УС – устройство сравнения; УК – устройство кодирования:

УОКК – устройство обработки контрольных кодов;

УД – устройство декодирования; Z – сигнал ошибки.

Избыточное кодирование основывается на введении во входной, обрабатываемый и выходной информационный сигнал дополнительных символов, которые вместе с основными образуют коды, обладающие свойствами обнаружения или исправления ошибок.

В качестве примера встроенного контроля с избыточным кодированием рассмотрим один из методов контроля передачи информации: к группе информационных разрядов, представляющих собой простой (т. е. неизбыточный) код добавляется один избыточный (контрольный) разряд, несущий информацию о четности и нечетности передаваемой информации. Значение разряда четности равно), если число единиц в передаваемом коде четное и 1, если число единиц нечетное (рис.2).

При передаче информации слово передается со своим контрольным разрядом. Если приемное устройство обнаруживает, что значение контрольного разряда не соответствует четности суммы единиц слова, то это воспринимается как признак ошибки в линии передачи информации.

+

+

+

Канал передачи информации

n

Z

n+1

Рис. 2. Передача информации с контрольным разрядом: если Z=0, то информация передается без ошибки; если Z=1, то информация передается неверно; n – число основных каналов; n+1 – дополнительный контрольный разряд.

По нечетности контролируется полное пропадание информации, так как кодовое слово, состоящее из нулей, относится к запрещенным.

Этот метод применяют в микропроцессорных системах для контроля передач информации между регистрами, считывания информации в ОЗУ, обменов между устройствами. Магистрали передач данных составляют от 60 до 80% всех аппаратных средств МПС. Поэтому использование контроля по четности позволяет существенно повысить надежность операций передачи информации.

=1

=1

=1

=1

=1

=1

=1

=1

1

2

3

4

5

6

7

8

Z

Х1

Х2

Z

Х1 Х2

0

1

0

1 1

0

1

1

0

Y

Z=0 –четное

Z=1 – нечетное

Рис. 3. Схема контроля четности-нечетности 8-миразрядной шины пирамидального типа на двухвходовых логических элементах "исключающее ИЛИ"

Другим примером могут явиться итеративные коды. Их применяют при контроле передач массивов кодов между внешним ЗУ и ЭВМ, между двумя ЭВМ и других случаях. Итеративный код образуется путем добавления дополнительных разрядов по четности к каждой строке и каждому столбцу передаваемого массива слов(двумерный код). Кроме того, четность может определяться и по диагональным элементам массива слова(многомерный) код. Обнаруживающая способность кода зависит от числа дополнительных контрольных символов. Он позволяет обнаружить многократные ошибки и прост в реабилитации.

К простейшим аппаратным способам встроенного контроля относится способ дублирования схем и сравнения выходных сигналов этих схем (рис.3). Этот метод легко можно применить для проверки любой схемы. Кроме тог, он обладает преимуществом, что может обнаружить любую функциональную ошибку, появляющуюся в схеме. Недостатком метода является во-первых – увеличение затрат на резервирование и, во-вторых – не исключение собственных ошибок резервной контрольной аппаратуры.

Несколько снизить затраты на аппаратное дублирование цифровых схем можно путем использования так называемой двухпроводной логики. При этом исходная и резервные схемы отличаются тем, что они реализуют инверсные выходы и в схеме все сигналы представлены одновременно в прямом и инвертируемом виде. Сравнение выходных сигналов при обычном дублировании осуществляется на основании их равенства, а при двухпроводной логике – на основании их неравенства.

Для обнаружения ошибок в комбинационных схемах, в особенности для арифметических и логических функций, зависящих от двух аргументов, часто применяют метод псевдодублирования. В этом случае данные обрабатываются дважды последовательно во времени, в одинаковом порядке, однако по различным путям и проверяются на равенство с использованием промежуточного запоминающего устройства. При этом вместо требуемого резервирования схемы фактически увеличивается время обработки информации.

На рис.4 изображена схема проверки двухразрядного покомпонентного логического объединения двух операндов при помощи АЛУ. Вначале переключатели S1 и S2 включаются в правое по схеме положение и с выхода АЛУ результат операции записывается в регистре 3 памяти, подключенных к одному из входов схемы сравнения.

На следующем шаге переключатели S1 и S2 включаются в левое положение. Старшие и младшие разряды входных чисел на входе АЛУ меняются местами, а результат операции с выхода АЛУ с также переставленными старшим и младшим разрядом поступает непосредственно на схему сравнения.

Рг 1

Рг 2

ОС

Рг 3

X1

X2

S1

4 3 2 1

4 3 2 1

АЛУ

4 3 2 1

S2

4 3 2 1

1

2

3

4

1

2

3

4

Рис. 4. Схема проверки выполнения арифметических операций по методу псевдодублирования

Допустим, что на выходе 3 АЛУ проявляется ошибка "=1" (тождественная единица) и операнды 0110 и 0010 поразрядно складываются в АЛУ по модулю 2. Если переключатели S1 и S2 включены в правое положение, то в регистр 3 записывается число 0100. Если переключатели включены в левое положение, т. е. на выходы АЛУ поступают числа 1100 и 0100, соответственно, а на выходе 1100 (с учетом ошибки =1 на выходе 3 АЛУ). На входы схемы сравнения поступают коды 0100 – с выхода регистра 3 и 0110 – с выхода АЛУ, которые вырабатывают сигнала ошибки.

Встроенный контроллер особенно удобен для организации контроля и диагностики изделий в условиях эксплуатации, но он может оказаться полезным и в производственных условиях, например, при изготовлении БИС микропроцессорных комплектов. Для этого в схему БИС вводятся дополнительные средства, осуществляющие реконфигурацию структуры БИС в режиме тестирования и обеспечивающие, при этом, улучшение управляемости и наблюдаемости всех, входящих в нее триггеров (рис.5, а). В этом случае тестирование сложной БИС превращается в сравнительно простую процедуру для рекомбинационных схем, входящих в БИС.

Для реализации такого подхода необходимы такие средства реконфигурации структуры последовательностной схемы, чтобы сигнал управления переключал все триггеры из рабочего режима в тестовый, при котором все триггеры становятся управляемыми и наблюдаемыми (рис.5, б). Наибольшее распространение среди этих методов получил метод сканирования \*\*\*\* осуществляемый за счет соединения специальных дополнительных элементов памяти в единый сдвиговый регистр, запоминающий внутренне состояние схемы. Сканирование дополнительных элементов памяти можно контролировать и путем адресации к ним и прямого выбора информации о состоянии схему из дополнительных ЗУ.

Все это усложняет БИС, однако обеспечивает экономическую целесообразность. Так для МП серии Intel 8086, имеющего площадь кристалла 3 мм2, введение средств повышения контролепригодности увеличивает площадь кристалла примерно на 20%, что снижает выход годных с 10% до 12(20)%. Вместе с уменьшением количества кристаллов на пластине это приводит к удорожанию производства на 70%. Тем не менее уменьшение стоимости тестирования, которое составляет более 80% трудоемкости изготовления БИС, полностью компенсирует такое удорожание БИС и сложные ПУ разрабатываются таким образом, чтобы обеспечить возможность самотестирования без участия внешнего оборудования и программных средств.

Для реализации самотестирования схем на печатной плате или на кристалле микропроцессора размещают два регистра, запрограммированных на выполнение функций генератора псевдослучайных кодов и сигнатурного генератора. В программируемом ПЗУ процессора храниться специальная тест-программа, которая должна обеспечить последовательное тестирование всех функциональных узлов микропроцессора. Генератор псевдослучайных кодов формирует входную тестовую последовательность, направленную в контролируемые программно-доступные блоки микропроцессора, а сигнатурный генератор снимает с выхода микропроцессора соответствующие контрольные сигнатуры которые в свою очередь сравниваются с эталонными, хранимыми в ПЗУ. Результат сравнения дает информацию микропроцессору о своем состоянии.

Самодиагностика БИС является естественным развитием структурного подхода к проектированию контролепригодных устройств. Сочетание встроенных средств контролепригодности (сквозного сдвигового регистра для сканирования состояний, генератора псевдослучайных тесткодов, регистра сигнатурного анализа) позволяет организовать самотестирование кристаллов, полупроводниковых пластин, микросхем и печатных узлов. Поскольку стоимость средств самодиагностирования остается примерно одинаковой, а затраты на тестирование стандартными методами увеличиваются в геометрической прогрессии, можно полагать, что с ростом насыщенности СБИС (степени интеграции) средства самодиагностики станут обязательными.

Рис. 5. Встроенный контроль БИС МП. Реконфигурация структуры БИС в режиме тестирования с использованием дополнительных триггеров (а) и специального ЗУ (б)

Комбинационная

схема

ЭП-1

ЭП-2

ЭП-N

Zm

Xn

Вход сканирования

Выход сканирования

Синхросигналы

а)

Комбинационная схема

Адресуемые

элементы

памяти

Y-дешифратор

Х-дешифратор

Адрес сканирования

б)

# ЛИТЕРАТУРА

1. Б. Хабаров, Г. Куликов, А. Парамонов. Техническая диагностика и ремонт бытовой радиоэлектронной аппаратуры. – Мн.: Издательство: Горячая Линия – Телеком, 2004. – 376 с.

2. Дэвидсон Г. Поиск неисправностей и ремонт электронной аппаратуры без схем.2-е издание.М. Издательство: ДМК Пресс. 2005, - 544 с.

3. Игнатович В.Г., Митюхин А.И. - Регулировка и ремонт радиоэлектронной аппаратуры. - Минск: "Вышэйшая школа", 2002 – 366 с.

4. Н.И. Домарёнок, Н.С. Собчук. "Физические основы диагностики и неразрушающего контроля качества МЭА", – Мн., БГУИР, 2001.