УДК 681.5

Верификация систем на основе цифровых СБИС с диверсификацией

Е.В. Таперова

ФГУП ВНИИА им. Духова, taperovaev@gmail.com

***Аннотация* — В докладе рассматривается методика, позволяющая верифицировать систему на основе цифровых СБИС, для которых применена диверсификация. Методика позволяет подтвердить выполнение частями системы одинаковых функций.**

***Ключевые слова* — диверсификация, верификация, конечный автомат, эталонная модель, функциональная эквивалентность.**

I. Введение

В областях промышленности, где отказы могут привести к масштабным техногенным катастрофам, разработчики обязаны ответственно подходить к методам управления рисками аварий. Одной из таких областей является атомная энергетика. Безопасность эксплуатации АЭС обеспечивается системой контроля и управления.

Части системы контроля и управления АЭС, выполняющие функции обеспечения безопасности (функции категории А), должны обладать резервированием, разделением и обеспечивать устойчивость к единичным отказам [1]. Одним из видов единичного отказа считается отказ по общей причине – отказ, явившийся результатом одного или более событий, вызывающих одновременный отказ двух или более отдельных каналов многоканальной системы или многоканальных систем, и приводящий к отказу системы (систем) [2]. Основным способом защиты от отказов по общей причине является принцип 3D - "diversity and defense of depth" (диверсификация и эшелонированная защита) [3]. Эшелонированная защита подразумевает использование нескольких барьеров, предотвращающих развитие аварии. Диверсификация обеспечивает логическое разделение, т.е. различные подходы к выполнению одинаковой функции обеспечения безопасности. Существующие параметры, которые определяют наличие и качество диверсификации, описаны в таблице 1 [3].

Системы контроля и управления (СКиУ) строятся в большинстве случаев на цифровых СБИС, так как обрабатывают значительные объемы информации и осуществляют сложные алгоритмы.

При проектировании таких систем необходимо подтверждение эквивалентности выполняемых диверсифицированными частями системы функций. Это связанно с тем, что при любом состоянии управляемой системы диверсифицированными частями управляющей системы должны формироваться управляющие воздействия, направленные на одинаковое изменение параметров управляемой системы. Причем это изменение параметров должно обеспечиваться непротиворечивой последовательностью действий.

Таблица 1

Параметры диверсификации

	СКиУ
Конструкция	
Различные технологии	
Различные технологические методы	
Различная архитектура	
Функции	
Различные управляемые механизмы	✓
Различные контролирующие системы	
Различное время отклика	✓
Устройство	
Различные производители принципиально разных устройств	
Принципиально разные устройства одного производителя	
Различные производители схожих устройств	
Схожие устройства одного производителя	
Сигналы	
Различные технологические параметры, идентифицируемые по различным физическим эффектам	✓
Различные технологические параметры, идентифицируемые по одинаковым физическим эффектам	✓
Одинаковые реакции на различные данные, полученные со схожих датчиков	✓
Человеческий фактор	
Конструкции различных организаций	
Конструкции различных частей организации	
Конструкции различных инженеров или программистов	
Различные тестеры и проверяющие	
Логика работы	
Различные алгоритмы, логика и архитектура программ	✓
Различное время исполнения и порядок обработки команд	✓
Различное время работы среды разработки	

Существует два подхода к верификации таких систем. Первый подход рассматривает управляющую и управляемую системы в целом. Для этого строятся

модель управляемой системы и модель управляющей системы, и проводится анализ их взаимодействия. Такой подход обеспечивает комплексную оценку свойств системы управления, но такое моделирование возможно только при рассмотрении готового проекта, то есть не применим на этапе разработки отдельных узлов управления для модульной системы. При разработке узлов управления модульной системы применяется второй подход, когда верификация каждой из диверсифицированных частей системы проводится независимо. Для каждой из частей формируются отдельные требования и тестовые воздействия. Оценка эквивалентности выполняемых функций проводится разработчиком умозрительно. Следовательно, применение второго подхода может привести к выявлению ошибок в процессе системного моделирования. Так как системное моделирование проводится для конкретного проекта, то, возможно, что ошибки не будут выявлены на ранних этапах постановки устройства в серийное производство.

Целью данной работы является формирование методики, позволяющей на основании моделей диверсифицированных частей системы подтвердить их функциональную эквивалентность путем совместного построения тестовых воздействий для диверсифицированных частей системы.

Так как при верификации должна быть рассмотрена только логика работы системы, не все параметры диверсификации могут оказать влияние на систему тестирования диверсифицированных частей. Те параметры, которые влияют на систему тестирования, отмечены в таблице 1.

II. Модель и верификация системы контроля и управления АЭС

A. Описание системы контроля и управления

Функционирование системы контроля и управления АЭС зависит от значений технологических параметров АЭС. В зависимости от принимаемых технологических параметров СКиУ формирует управляющие команды на исполнительные механизмы. Под воздействием управляющих команд исполнительные механизмы меняют свое состояние, вследствие этого изменяются и технологические параметры, описывающие состояние АЭС. Задача СКиУ сводится к достижению требуемых значений технологических параметров и их поддержанию в допустимых пределах.

Начальное состояние СКиУ можно охарактеризовать начальными технологическими параметрами, а конечное – требуемыми технологическими параметрами. Для изменения технологических параметров исполняется последовательность команд, формируемых СКиУ, которые поступают на исполнительные механизмы. При этом каждой следующей команде соответствует достижение определенных контрольных значений для функции, зависящей от технологических параметров.

Система контроля и управления реализуется на одной или нескольких СБИС.

B. Выбор метода верификации

Для верификации модели СБИС используются формальная и динамическая верификации. Проверка соответствия логической схемы СБИС спецификации осуществляется путем анализа логической схемы. При динамической верификации происходит формирование наборов тестовых воздействий и ожидаемых выходных реакций. Более подробно каждый из подходов описан в [4], [5].

При верификации диверсифицированной системы можно выделить две основные задачи – автоматизированная верификация диверситетов и контроль функциональной эквивалентности.

Для автоматизированной верификации диверситетов могут быть использованы любые известные методы, тогда как для обеспечения возможности сравнения необходимо выбрать подход, при котором функционирование моделей легко сравнимо.

Одним из способов, позволяющих проводить контроль функциональной эквивалентности систем, является сравнение их представлений в виде конечных автоматов. Для проведения верификации системы может быть использована эталонная модель, представляющая собой конечный автомат. Такое описание позволяет выполнить требование и по автоматизированной верификации диверситетов [6].

C. Автоматическая генерация тестовых воздействий и проверка

Тестовые воздействия для автомата состояний характеризуются следующими метриками:

- метрика покрытия состояний,

- метрика покрытия переходов,

- метрика покрытия цепей длины k [7].

Количество входных воздействий при полном переборе равно количеству элементов множества цепочек входных воздействий. При большом количестве входных воздействий реализация их полного перебора может оказаться невозможной из-за временных ограничений.

Для конечного автомата может быть построен регулярный язык (по теореме Клини), для которого конечный автомат является распознающей моделью. Полный перебор значащих цепочек позволяет обеспечить покрытие всех состояний и переходов. Дополнение регулярного языка используется не полностью, применяются цепочки, отличающиеся от значащих на один символ алфавита. Значащими в данном случае называются такие цепочки, где переход между состояниями по одному внешнему воздействию осуществляется не более одного раза.

Построение системы тестовых воздействий обеспечивается решением задачи о перечислении путей [9], при котором не значащие пути откидываются. Значащие цепочки используются для построения дополнений.

Для проведения тестирования на основе эталонной модели используется стандартная архитектура тестовой системы на основе эталонной модели [8].

III. Верификация системы с диверсификацией

Для верификации функциональной эквивалентности предлагается подход, который основан на использовании эталонных моделей, описанных в виде конечных автоматов. Каждый из рассматриваемых принципов диверсификации был формализован в терминах теории конечных автоматов.

В результате было показано, что для подтверждения функциональной эквивалентности между диверсифицированными частями системы достаточно подтвердить, что входные и выходные языки конечных автоматов, соответствующие каждому из диверситетов, могут быть отображены друг в друга и при этом отображении функции совпадают.

Для решения задачи поиска соответствия между языками предложено использование конечных подстановок между входными языками диверсифицированных частей системы и между выходными языками диверсифицированных частей системы.

Верификация на основании эталонных моделей возможна, так как верификация каждого из диверситетов подтверждает соответствие между диверситетом и эталонной моделью в интересующей области значений.

A. *Функциональная эквивалентность конечных автоматов*

При переходе к рассмотрению эталонных моделей, представленных в виде конечных автоматов, необходимо сформулировать правила функциональной эквивалентности конечных автоматов.

Воспользуемся утверждением, что в том случае, если языки автоматов эквивалентны, то автоматы эквивалентны по определению.

Рассмотрим два конечных автомата: M_1 с языком $L_1(M_1)$ и M_2 с языком $L_2(M_2)$; такие, что конечные автоматы эквивалентны.

Применим к конечному автомату M_2 каждый из возможных подходов к диверсификации в терминах конечных автоматов.

Диверсификация сигналов

1) Различные технологические параметры, идентифицируемые по различным физическим эффектам и одинаковым физическим эффектам. Данные группы объединены, так как для системы физический эффект не влияет на восприятие информации.

С точки зрения логического автомата есть основной алфавит возможных событий на АЭС A с набором цепей A*, над которым стоит язык L, который соответствует возможным последовательностям событий, происходящим на АЭС. Существует алфавит возможных значений одного принимаемого параметра – A_1 и алфавит другого принимаемого параметра – A_2, а A^*_1 и A^*_2 наборы цепей. Для каждого слова из L найдется слово из A^*_1 t_1: $L \rightarrow A^*_1$ и слово из A^*_2 t_2: $L \rightarrow A^*_2$, которые являются его отображением, назовем их L_1 и L_2. Исходя из свойств транзитивности отображений языка получаем, что каждому слову из L_1 можно найти соответствующее ему слово из L_2 $t_{12}: L_2 \rightarrow L_1$ и наоборот $t_{12}^{-1}: L_1 \rightarrow L_2$. Правило, позволяющее найти соответствие между словами, назовем функцией перевода.

2) Использование нескольких резервированных датчиков – $L_1 = L_2$, значит конечные автоматы эквивалентны по определению.

Логическая диверсификация

1) Различные алгоритмы, логика и архитектура программ.

Введем отображения h_1: $A^*_1 \rightarrow A^*_{w1}$; h_2: $A^*_2 \rightarrow A^*_{w2}$. Заметим, что при одинаковых L_1 и L_2, а также L_{w1} и L_{w2}, получаем, что автоматы совпадают, т.е. эквивалентны, следовательно, их минимизированные формы также совпадают.

2) Различное время и порядок обработки внешних воздействий.

Подразумевается, что системы срабатывают в различные моменты времени после одного и того же воздействия. Языкам L_1=L_2 соответствуют начинающиеся в разный момент выходные реакции, при этом надо заметить, что момент окончания реакции должен совпадать, но в целом можно считать, что $h_1(L_1) = L_{w1}$, $h_2(L_1) = L_{w2}$.

Функциональная диверсификация

1) Различные управляемые механизмы.

С точки зрения логического автомата с выходом выходные воздействия должны быть направлены на одинаковое изменение состояния станции, а значит соответствовать языку L возможных последовательностей событий. При этом накладывается ограничение, которое требует, чтобы происходили одинаковые изменения по одному и тому же пути. Исходя из этого получаем, что существуют устройства, выполняющие одинаковую операцию и управляемую различными языками. Цепи управления одним устройством – A^*_{w1}, язык управления другим устройством – A^*_{w2}. Язык управления операцией – L_w. Аналогично предыдущему t_{w1}: $L_w \rightarrow A^*_{w1}$ и t_{w2}: $L_w \rightarrow A^*_{w2}$ назовем L_{w1} и L_{w2}, соответственно, $t_{w12}: L_{w2} \rightarrow L_{w1}$.

2) Различные длительности реакции.

Подразумевается, что переход из одного состояния в другое для различных частей системы может иметь разную длительность.

Данный принцип диверсификации характеризуется тем, что разным входным воздействиям для разных автоматов $t_{12}: L_2 \rightarrow L_1$ соответствуют одинаковые выходные реакции $L_{w2} = L_{w1}$, причем, $A_1 = A_2$, а значит $h_1(L_1) = L_{w1}$, $h_2(L_2) = L_{w1}$.

Из вышеприведенных данных следует, что функционально эквивалентными можно называть автоматы, которые удовлетворяют требованию существования функции перевода: L_1 в L_2 и L_{w1} в L_{w2}.

Значит h_1: $t_{12}(L_2) \rightarrow t_{w12}(L_{w2})$ и h_2: $t_{12}^{-1}(L_1) \rightarrow t_{w12}^{-1}(L_{w1})$

B. Верификация эталонных моделей системы диверсифицированных частей

Необходимо определить, являются ли автоматы функционально эквивалентными по определению, то есть удовлетворяют ли требованиям, указанным в пункте А данного раздела.

При доказательстве необходимо определить функции перевода входных языков и выходных языков. Для этого необходимо определить конечную подстановку.

Пара моделей СБИС – модель диверситета А и модель диверситета Б, для эталонных моделей которых определены функции перевода входных языков и функции перевода выходных языков, могут быть верифицированы с точки зрения функциональной эквивалентности.

Методика верификации показана на рисунке 1.

Для эталонных моделей ранее были сформированы тестовые воздействия. Заданный набор тестовых воздействий может быть преобразован с помощью функции перевода из тестовых воздействий модели А в тестовые воздействия модели Б. Тестовые воздействия модели А в непреобразованной форме передаются на модель А. Преобразованные в формат модели Б тестовые воздействия передаются на модель Б. На выходе модели А формируются выходные реакции, которые, как было подтверждено ранее, соответствуют выходным реакциям эталонной модели. Выходные воздействия модели А преобразуются с помощью функции перевода в выходные воздействия модели Б. На выходе модели Б формируются выходные реакции на переведенные тестовые воздействия модели А. Анализатором происходит сравнение переведенных реакций модели А с реакциями модели Б, при этом происходит, при необходимости, соответствующая задержка.

Переведенные в формат модели Б тестовые воздействия модели А сравниваются качественно и количественно с тестовыми воздействиями модели Б.

Верификация для второй части диверсифицированной системы происходит симметрично.

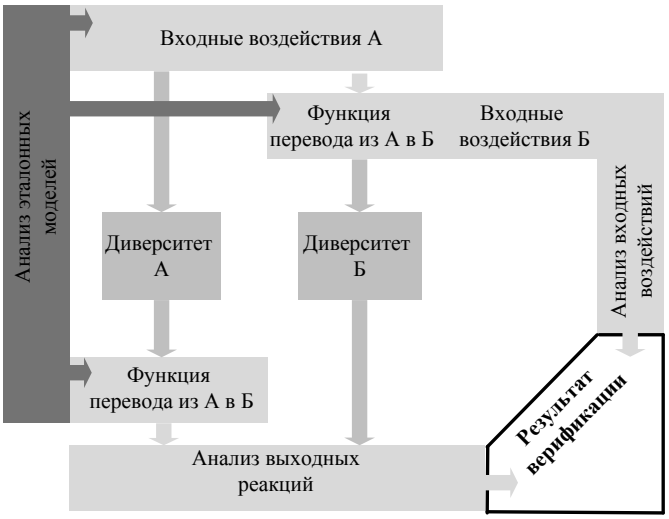


Рис. 1. Методика верификации

IV. Методика верификации

Для верификации диверсифицированной системы стандартная методика с использованием эталонной модели в виде конечного автомата [7] должна быть дополнена следующими этапами:

- построение функции перевода между входными воздействиями диверситетов и выходными реакциями диверситетов;

- проверка функциональной эквивалентности эталонных моделей путем минимизации с учетом функций перевода;

- верификация функциональной эквивалентности моделей.

Методика верификации в целом представляет собой следующую последовательность действий:

- построение эквивалентных конечных автоматов для диверсифицируемых частей системы;

- формирование тестовых воздействий;

- подтверждение соответствия тестируемых моделей эталонным;

- построение функции перевода между входными воздействиями диверситетов и выходными реакциями диверситетов;

- проверка функциональной эквивалентности эталонных моделей путем минимизации конечных автоматов с учетом функций перевода;

- верификация функциональной эквивалентности моделей.

При таком подходе к верификации длительность тестирования возрастает примерно в два раза по сравнению с раздельной верификацией. Время верификации можно сократить в два раза при проведении одновременного сравнения с эталонной моделью, но такой подход затрудняет отладку.

Если каждый из диверситетов может быть разделен на функциональные узлы, то для пар функциональных узлов из двух диверситетов, которые выполняют одинаковые функции, может быть проведена автономная верификация. При этом система является суперпозицией функциональных узлов.

V. Пример реализации методики

Рассмотрим верификацию системы из процессора (диверситет А) и ПЛИС (диверситет В), определяющих одно событие по различным параметрам.

Рассматривается пример применения данного подхода на примере САПР SCADE и без применения САПР системного проектирования.

A. Описание функций диверситетов

При наступлении исходного события на диверситет А датчиком формируется активный сигнал, характеризующий наступление события. Считается, что событие продолжается пока на входе присутствует активный сигнал.

Диверситет Б получает импульсы от датчика при наступлении и по окончанию событий.

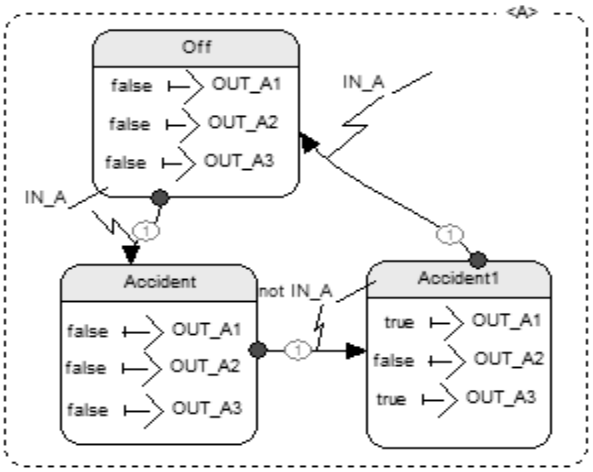
На протяжении того времени, когда существует исходное событие, диверситет А формирует на выходной каскад параллельный код, диверситет Б – импульсы определенной внешним воздействием частоты.

B. Формирование эталонных моделей

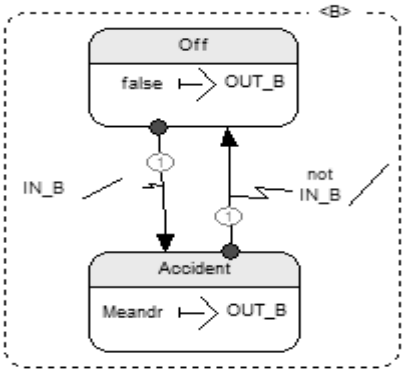
Для каждого из диверситетов в SCADE Suite происходит построение соответствующего ему конечного автомата – эталонной модели.

Модель на рисунке 2а соответствует диверситету А. Модель на рисунке 2б соответствует диверситету Б.

Модели также могут быть сформированы в виде таблицы транзакций в текстовом формате.



а



б

Рис. 2. Автоматы эталонных моделей

C. Формирование функций перевода

Формирование функций перевода осуществляется инструментом, описанным на языке Perl.

Инструмент позволяет автоматически формировать требуемую информацию о функциях перехода в текстовом формате из текстового описания или отчета-описания SCADE Suite.

В результате для функционально идентичных автоматов формируются:

- регулярные выражения, описывающие входной и выходной языки конечных автоматов, соответствующих эталонным моделям диверситетов;
- конечные подстановки между регулярными языками.

Для тех конечных автоматов, где конечные подстановки невозможны, формируются:

- регулярные выражения, описывающие входной и выходной языки конечных автоматов, соответствующих эталонным моделям диверситетов;
- список воздействий, для которых не найдены отображения.

В случае невозможности отображения между языками конечных автоматов необходимо вернуться к начальному этапу разработки алгоритма.

D. *Формирование тестовых воздействий и ожидаемых выходных реакций*

Формирование тестовых воздействий и ожидаемых реакций осуществляется инструментом, описанным на языке Perl.

Инструмент позволяет автоматически формировать требуемую информацию о тестовых воздействиях из текстового описания или отчета-описания SCADE Suite.

Для каждого автомата формируются:

- тестовые цепочки с конфигурируемым параметром глубины зацикливания и пустыми переходам в текстовом формате и в формате HDL-описания;
- ожидаемые выходные реакции на тестовые воздействия в текстовом формате.

HDL-описание является тестовой оболочкой для моделирования в среде MG ModelSim.

E. *Построение описаний для СБИС*

В результате по описанным моделям строится описание функционирования для процессора (языки C, Assembler) и для ПЛИС (на HDL-языке). В случае использования SCADE Suite и GENCODE код HDL и код C может быть сгенерирован автоматически.

F. *Преобразование тестовых воздействий и выходных реакций*

При верификации в SCADE Suite формируется система тестирования, изображенная на рисунке 1.

Функции перевода автоматически генерируются из текстовых файлов, полученных в пункте C. Тестовые воздействия автоматически формируются из текстовых файлов, полученных в пункте D.

В данном случае верификация может быть проведена в полном соответствии с традиционным подходом верификации с эталонной моделью.

В процессе тестирования формируются текстовые файлы с данными о покрытии тестами модели.

Если выходные реакции в диверситетах не совпадают, то формируется выходной файл, содержащий последовательность входных воздействий, последовательности выходных реакций, последовательность эталонных реакций.

При верификации без использования SCADE преобразование происходит на уровне текстовых файлов. Верификация в случае применения моделей может быть проведена в САПР MG ModelSim. В случае невозможности проведения моделирования верификация может быть проведена в составе оборудования при помощи САПР NI LabView. Также возможна смешанная верификация. В этом случае происходит сравнение ожидаемых выходных реакций с выходными реакциями с учетом временных характеристик, их совпадение является критерием корректного функционирования.

VI. Заключение

Описанная методика верификации предназначена для верификации узлов модульной системы на базе цифровых СБИС, в которых используется диверсификация. Предложены дополнительные процедуры, которые позволяют автоматически подтвердить функциональную эквивалентность диверсифицированных частей системы на этапе проектирования.

Методика позволяет, построив эталонную модель системы или ее части в формате конечного автомата, автоматически выполнить верификацию системы и провести локализацию несоответствий.

Данная методика была применена для верификации модуля приоритетного управления АСУТП ТПТС-ЕМ.

Литература

[1] ГОСТ Р МЭК 62340:2007 Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине [IEC 62340:2007 "Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure"].

[2] ГОСТ Р МЭК 61513-2011 Системы контроля и управления, важные для безопасности. Общие требования (IEC 61513:2001 "Nuclear power plants - Instrumentation and control important to safety - General requirements for systems").

[3] Diversity strategies for Nuclear Power Plant Instrumentation and Control System, NUREG/CR-7007, U.S. NRC, Washington, DC. February 2010.

[4] Пантелеев А., Литвинов Е. Верификация и тестирование сложнофункциональных СБИС // Электронные компоненты. 2012. № 6.

[5] Bergeron J. Writing testbenches: functional verification of HDL models. Kluwer Academic Publishers. 2003. 479 p.

[6] Подъячев А.Ю. Использование метода покрытий при верификации моделей IDEF-0 // Труды СПИИРАН. СПб.: Наука, 2007. Вып. 5.

[7] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Использование конечных автоматов для тестирования программ // Программирование. 2000. № 26(2). С. 61-73.

[8] Wile B., Goss J.C., Roesner W. Comprehensive functional verification the complete industry cycle. CA: Morgan Kaufmann Publishers. 2005. 676 p.

[9] Белоусов А.И., Ткачев С.Б. Дискретная математика: Учеб. для вузов / под ред. В.С. Зарубина, А.П. Крищенко. 3-е изд., стереотип. М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. 744 с.